Installation Guide

Wyse Device Manager™ Release 4.9.1

Issue: 042012
PN: 883886-01 Rev. N

Copyright Notices

© 2012, Wyse Technology Inc. All rights reserved.

This manual and the software and firmware described in it are copyrighted. You may not reproduce, transmit, transcribe, store in a retrieval system, or translate into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, any part of this publication without express written permission.

End User License Agreement (“License”)

A copy of the Wyse Technology End User License Agreement is included in the software and provided for your reference only. The License at http://www.wyse.com/license as of the purchase date is the controlling licensing agreement. By copying, using, or installing the software or the product, you agree to be bound by those terms.

Trademarks

The Wyse and PocketCloud logos and Wyse and PocketCloud are trademarks of Wyse Technology Inc. Other product names mentioned herein are for identification purposes only and may be trademarks and/or registered trademarks of their respective companies. Specifications subject to change without notice.

Restricted Rights Legend

You acknowledge that the Software is of U.S. origin. You agree to comply with all applicable international and national laws that apply to the Software, including the U.S. Export Administration Regulations, as well as end-user, end-use and country destination restrictions issued by U.S. and other governments. For additional information on exporting the Software, see http://www.microsoft.com/exporting.

Ordering Information

For availability, pricing, and ordering information in the United States and Canada, call 1-800-GET-WYSE (1-800-438-9973) or visit us at **wyse.com**. In all other countries, contact your sales representative.

Contents

1 Introduction *1*

About this Guide *2*
- Finding the Information You Need in this Guide *2*

Wyse Technical Support *2*
- Related Documentation and Services *2*
- Wyse Online Community *2*

2 Preparing for Installation *3*

Pre-Installation Checklist *3*
Hardware Requirements *6*
Software Requirements *6*
Communication Port Requirements *7*
Upgrading Requirements *8*
Requirements for Managing PCoIP Devices *9*
- Creating a DNS Service Location (SRV) Resource Record for Wyse ThreadX Devices *9*

3 Installing or Upgrading WDM Workgroup Edition *11*

Installing or Upgrading Procedures (WDM Workgroup Edition) *12*

4 Installing or Upgrading WDM Enterprise Edition *15*

About Evaluation Licensing *16*
Installing or Upgrading Procedures (WDM Enterprise Edition) *16*
- Detailed Custom Installation and Upgrade Instructions *19*
  - WDM Database Installation Tips You Need to Know *20*
  - Software Repository Installation Tips You Need to Know *22*
  - Administrator Console Installation Tips You Need to Know *24*

A Activating Your Sales Key *25*

B Uninstalling WDM *27*

C Reference and Troubleshooting: FTP, IIS, and Firewall Information *29*

How the WDM Installer Installs and Configures FTP *30*
- Installing and Configuring FTP on Windows Server 2008 *30*
- Installing and Configuring FTP on Windows Server 2008 R2 *34*
- Installing and Configuring FTP on Windows 7 *37*

How the WDM Installer Installs and Configures IIS *40*
- Installing IIS 7.0 on Windows Server 2008 *40*
  - Installing WebDAV Extension for IIS 7.0 *42*
  - Configuring the Web.config File *42*
- Installing IIS 7.5 on Windows Server 2008 R2 *43*
- Installing IIS 7.5 on Windows 7 *46*

Using Windows Firewall with WDM *49*

Tables *51*

This page intentionally blank.

1 Introduction

Wyse Device Manager™ (WDM) software is the premier enterprise solution for managing network intelligent devices simply, remotely, and securely. It enables IT professionals to easily organize, upgrade, control, and support thousands of devices running Microsoft Windows XP Embedded, Microsoft Windows CE, Wyse Enhanced Microsoft Windows Embedded Standard, Wyse Enhanced Microsoft Windows Embedded Standard 7, Wyse Enhanced SUSE Linux Enterprise, Wyse ThinOS, Wyse Xenith, or ThreadX across any LAN, WAN, or wireless network.

WDM software uses industry standard communication protocols and a component-based architecture to efficiently manage your network devices. Its intuitive, simple, and powerful user interface is built to operate as a standard snap-in to the Microsoft Management Console (MMC). From one simple to use console, WDM allows you to manage all of your network devices easily and quickly.

Tip

For information on configuring WDM to securely manage your Wyse cloud clients and zero clients (with general guidance and specific instructions on configuring WDM and Wyse devices for secure management), refer to Wyse Knowledge Base Solution **#22428** (go to the Wyse Knowledge Base at http://www.wyse.com/kb and search for **22428**).

About this Guide

This guide provides the step-by-step instructions you need to install and configure a WDM environment. It also includes the requirements you must address before you begin the installation procedures.

This guide is intended for experienced network administrators and Information Technology professionals who have installed and configured Windows operating systems and applications.

Finding the Information You Need in this Guide

You can use either the Search window or Find toolbar to locate a word, series of words, or partial word in an active PDF document. For detailed information on using these features, refer to the Help in your PDF reader.

Wyse Technical Support

To access Wyse technical resources, visit http://www.wyse.com/support. If you still have questions, you can submit your questions using the Wyse Self-Service Center at http://support.wyse.com/selfservice.html or call Customer Support at 1-800-800-WYSE (toll free in U.S. and Canada). Hours of operation are from 6:00 A.M. to 5:00 P.M. Pacific Time, Monday through Friday.

To access international support, visit http://www.wyse.com/global.

Related Documentation and Services

Wyse Device Manager features can found in the Wyse Device Manager Datasheet. It is available on the Wyse Web site at: http://www.wyse.com/products/software/management/WDM.

Administrators Guide: Wyse Device Manager™ is intended for administrators of the WDM system. It provides information and detailed system configurations to help you design and manage a WDM environment.

Wyse Cloud Software is available on the Wyse Web site at: http://www.wyse.com/products/software.

Wyse Online Community

Wyse maintains an online community where users of our products can seek and exchange information on user forums. Visit the Wyse Online Community forums at: http://community.wyse.com/forum.

2 Preparing for Installation

This chapter contains the pre-installation requirements you must complete to prepare the environment for WDM installation and configuration. After you have completed all pre-installation requirements, you can continue with the installation/upgrade you want ("Installing or Upgrading WDM Workgroup Edition" or "Installing or Upgrading WDM Enterprise Edition").

Pre-Installation Checklist

Before you begin installing WDM, be sure you have met the following requirements:

- Refer to the WDM Release Notes for changes in this version of WDM. WDM 4.9.1 adds additional security features that enhance secure management of your Wyse devices. Use of WDM 4.9.1 requires that you install/upgrade to the latest WDM agents (HAgents) included in WDM 4.9.1 (see WDM Release Notes for more details).
- Obtain and configure all hardware and software, as necessary (see "Hardware Requirements" and "Software Requirements"). **CAUTION:** It is required that you *do not* install WDM on any server which is currently dedicated to other tasks (such as a Domain Controller, Backup Controller, Mail Server, Production Web Server, DHCP Server, MSMQ Server, Application Server, and so on). It is highly recommended that WDM be installed on a server that is dedicated to WDM services.
- Install a supported operating system on the machine to which WDM will be installed. Be sure that all systems are up-to-date with current Microsoft service packs, patches, and updates (see "Software Requirements").
- Install Microsoft Internet Explorer (IE) 6.0 or later on all machines.
- Use of the built-in HTML help files requires Java to be installed on all machines to which you install the WDM Administrators Console (**MMC Snap-in**). Visit http://www.java.com and install the latest Java/JRE version for your operating system).
- If you are running IIS 7.0 on Windows Server 2008 SP1 or IIS 7.5 on either Windows Server 2008 R2 or Windows 7, be sure to update the HAgent on your devices to the latest WDM agents (HAgents) included in WDM 4.9.1 (see WDM Release Notes for more details) to ensure your devices are discovered by WDM (otherwise, IIS limitations may prevent discovery).
- Ensure that no other applications requiring IIS are running on the machine to which WDM will be installed.
- Ensure that all required communications ports are available and open for proper communication between servers, routers, and switches (see "Communication Port Requirements").
- Ensure you have access to your operating system CD-ROM and your Microsoft Windows system files for use during your installation. **NOTE:** During WDM installation WDM checks the system to determine if all required software is present. If required software is not present, WDM indicates which software is missing. Some required third-party software is included with the WDM software, while other software is available from your operating system CD-ROM or from the network location for your Microsoft Windows system files (usually the i386 folder).

- *WDM Workgroup Edition Only*:
  - You do not need to obtain special licenses to install WDM (you will use the WDM *Workgroup Sales Key* that appears by default in the *InstallShield Wizard*).
  - Ensure your FTP service is running (see also "How the WDM Installer Installs and Configures FTP"). Note that you can ignore all HTTP/HTTPS information in this guide, as you must use FTP.
  - Ignore all WebDAV for Microsoft Windows information in this guide (you do not need WebDAV for Microsoft Windows).
  - Ignore all custom SQL Server information in this guide (you must use Microsoft SQL Server 2008 R2 Express (32-bit) which WDM installs by default).
- *WDM Enterprise Edition Only*:
  - Ensure you obtain (from Wyse) and have access to your WDM *Enterprise Sales Key* or *Enterprise Evaluation License Key* for use during your installation (after purchase, you should have received an email from Wyse or your reseller with full instructions on registering and generating your WDM *Enterprise Sales Key*; if you did not receive this email, contact your reseller).
  - WDM requires a supported SQL Server as described in "Software Requirements." WDM provides (and installs) Microsoft SQL Server 2008 R2 Express (32-bit) as the default option, however, you can choose to use another supported SQL Server. To use another supported SQL Server, you must perform a *Custom* installation (see "Installing or Upgrading Procedures (WDM Enterprise Edition)").
  - If you plan to install and configure WDM components on multiple machines (*Custom* installation), you will repeat some of the installation and configuration procedures in this guide. Likewise, you must also complete the pre-installation requirements for each related machine you intend to use.
  - If you plan to use FTP, ensure your FTP service is running (see also "How the WDM Installer Installs and Configures FTP"). **CAUTION:** If you intend to use the firmware upgrade feature for Wyse ThreadX devices, FTP must be configured.
  - If you plan to use HTTP or HTTPS for your server communications, you *must* perform a custom installation (see "Detailed Custom Installation and Upgrade Instructions"). In addition the WDM installer will install WebDAV for Microsoft Windows on IIS and use the HTTP or HTTPS ports (as described in "Communication Port Requirements").

Caution

(*Installations on Windows Server 2008 Only*) - During the installation, if you are prompted to download and install the WebDAV Extension for IIS 7.0, simply follow the instructions (see also "Installing WebDAV Extension for IIS 7.0").

  - If you plan to use Wyse ThreadX devices, you must create and configure a DNS Service Location (SRV) resource record as described in "Requirements for Managing PCoIP Devices."

- *Upgrading Current WDM Installations Only:*
  - *Planning for Upgrading* - **WDM 4.9.1 supports an upgrade from WDM version 4.9.0 *ONLY*. You cannot upgrade from any other version.**
    IMPORTANT: **After upgrading to WDM 4.9.1, you *must* upgrade all devices with the latest HAgent packages available to ensure your devices can be managed using WDM. Be sure to consult the latest WDM Release Notes.**
    WDM 4.9.0 supports direct upgrades from WDM version 4.8.0, or 4.8.5. If you are running WDM version 4.7.0 or 4.7.1, you must first upgrade to 4.7.2, and then upgrade to 4.8.5 *before* upgrading to 4.9.0. **CAUTION:** Upgrading from WDM 4.7.2 to 4.8.5 is supported if the following hotfixes are installed in the following order *prior* to installing WDM 4.8.5: HF04072025609 and then HF04072036209.
  - *WDM 4.7.2 Installations Planning for V90L, V90LE, or V90LEW Devices Using Non-PXE Imaging* - If you have an existing WDM 4.7.2 installation containing V90L, V90LE, or V90LEW devices, and you want to continue using Non-PXE imaging in WDM 4.9.0, be aware of the following requirements *before* upgrading to WDM 4.9.0 (**CAUTION:** If you have devices running earlier builds than those described below, you must re-image the devices with the latest firmware *before* you upgrade to WDM 4.9.0):
    - If you have V90L and V90LE devices running XPE build 673 or later, you must *first* upgrade your devices using the following package (obtained from Wyse) *before* upgrading to WDM 4.9.0: *MerlinBootAgentUpgradeXPE_VLE.zip*
    - If you have V90LEW devices running WES build 688 or later, you must *first* upgrade your devices using the following package (obtained from Wyse) *before* upgrading to WDM v4.9.0: *MerlinBootAgentUpgradeWES_VLE.zip*

Hardware Requirements

Depending on your operating system, be sure the machine(s) to which you will install WDM meets or exceeds the minimum system requirements shown in Table 1 for 32-bit operating systems or in Table 2 for 64-bit operating systems (as these are general guidelines, be sure to refer to your operating system documentation for details on hardware requirements).
IMPORTANT: The actual free space required depends on the number and size of the packages you register, as well as the number of devices you will be managing (the WDM Database size). The minimum free space shown assumes the WDM Database and packages require that amount of space.

Table 1 Server Hardware Requirements for 32-bit OS

Category	Minimum Requirements	Recommended
CPU	1GHz Intel or AMD X86	2.4 GHz Dual Core Intel or AMD X86
RAM	2 GB	4 GB
Minimum Free Space	4 GB	20 GB

Table 2 Server Hardware Requirements for 64-bit OS

Category	Minimum Requirements	Recommended
CPU	1GHz Intel or AMD X86	2.4 GHz Dual Core Intel or AMD X86
RAM	4 GB	8 GB
Minimum Free Space	8 GB	40 GB

Software Requirements

WDM 4.9.1 supports the English versions of software shown in Table 3. Installing the latest version of each software package is highly recommended.

Table 3 Server Software Requirements

Component	Software Requirements
Operating System	Windows Server 2008 R2 (64-bit) Windows Server 2008 R2 SP1 (64-bit)
Database Server	Microsoft SQL Server 2005, 2005 Express, 2008, 2008 Express, or 2008 R2 Express (32-bit)

By default, WDM installs Microsoft SQL Server 2008 R2 Express (32-bit). To use an SQL Server Personal Edition, SQL Server Developer Edition, or another supported SQL Server, you must perform a custom installation (see "Installing or Upgrading Procedures (WDM Enterprise Edition)").

Communication Port Requirements

To perform their full range of management functions, WDM software components require certain ports to remain open on your servers, routers, and switches.

For example, WDM relies on the HTTP/HTTPS communications port designated by your Web service (such as Microsoft Internet Information Service) for push operations (push refers to operations initiated by WDM and sent/pushed to devices). Push operations include:

- Issuing quick device commands (such as Refresh Device Information, Reboot, Change Device or Network Information, Get Device Configuration, and so on)
- Distributing packages at a specific time (either immediately or at a specific date and time)

Typically, port 80 is designated as the HTTP port and port 443 is designated as the HTTPS port. However, if port 80 (or the designated HTTP port), or port 443 (or the designated HTTPS port) is closed, WDM will be unable to push updates or quick commands to devices.

Table 4 lists the ports WDM uses and describes the respective communication protocols and their function (ensure that these ports are open for proper communication between servers).

Table 4 Communication Ports

WDM Component	Protocol	Port	Function
GUI	HTTP	80 280	Communicate with the Web Service and Standard Service.
	FTP	21	Register new packages into the Master Software Repository.
	OLE DB	1433 (default) Can be configured during installation	Communicate with the WDM Database.
	VNC	5800 5900	Remote shadows devices.
Web Service	HTTP	80 280	Communicate with the Web Agent, GUI, and Standard Service.
	HTTPS	443 8443	Secure Communication with the Web Agent, GUI, and Standard Service
	OLE DB	1433 (default) Can be configured during installation	Communicate with the WDM Database.
Web Agent	HTTP	80 280	Communicate with the Web Service.
	FTP	21	Read and write files to the Master and Remote Software Repositories.

Table 4 Communication Ports, Continued

WDM Component	Protocol	Port	Function
Standard Service	OLE DB	1433 (default) Can be configured during installation	Communicate with the WDM Database.
	HTTP	8008	Communicate with the GUI and Web Service.
Standard Service and PXE	DHCP	67 68 4011	Process UDP requests from PXE-enabled devices to the Standard Service.
	TFTP	69	Download bootable image to enable management processing.
	HTTP	80	Communicate with the Web Service regarding actions and status of current task.
	FTP	21	Download and upload files to the Master and Remote Software Repositories.
Standard Service and legacy support for older WDM Agents	UDP	44956 44957	Discover devices (using subnet directed broadcasts) that have older WDM Agents (5.0.0.x and earlier) installed.
	TCP	44955	Discover devices using IP Range Walking. Upgrade devices that have an older WDM Agent (5.0.0.x and earlier) installed.
ThreadX Manager Service	TCP	9880 50000	Uses these ports to communicate with ThreadX devices.

Upgrading Requirements

WDM 4.9.1 supports an upgrade from WDM version 4.9.0 *ONLY*. You cannot upgrade from any other version.
***IMPORTANT*: After upgrading to WDM 4.9.1, you *must* upgrade all devices with the latest HAgent packages available to ensure your devices can be managed using WDM. Be sure to consult the latest WDM Release Notes.**
WDM 4.9.0 supports direct upgrades from WDM version 4.8.0, or 4.8.5. If you are running WDM version 4.7.0 or 4.7.1, you must first upgrade to 4.7.2, and then upgrade to 4.8.5 *before* upgrading to 4.9.0.

Caution

Upgrading from WDM 4.7.2 to 4.8.5 is supported if the following hotfixes are installed in the following order *prior* to installing WDM 4.8.5: HF04072025609 and then HF04072036209.

Requirements for Managing PCoIP Devices

PCoIP devices (running ThreadX firmware) require a DNS Service Location (SRV) resource record to perform the following actions:

- **Partial Check-In (heartbeat)** - Where the device performs a heartbeat check-in every 5 minutes (this amount of time is not configurable).
- **Firmware Download Completion Status** - Where firmware upload is initiated by the server and download completion is initiated (made known) by the device using the DNS SRV record.
- **Reboot Status** - This necessary intimation (especially when DHCP lease for an IP has expired and a device receives a fresh IP) enables WDM to keep track of the device even if an IP has changed.

Therefore, it is *highly recommended* to complete the steps in "Creating a DNS Service Location (SRV) Resource Record for Wyse ThreadX Devices."

However, for special cases where a DNS server is unavailable, you can provide a polling mechanism where WDM runs a polling thread to check if the ThreadX devices listed in the Device Manager are up and running. Simply enable the ThreadX device polling feature (**Device Configuration > Preferences > Service > Enabling ThreadX Device Polling**) and then restart the ThreadX Service. **CAUTION**: Be aware that this polling thread is *not* equivalent to using a DNS Service Location (SRV) resource record and is a workaround to manage only a *Partial Check-In (heartbeat)*. *Firmware Download Completion Status* and *Reboot Status* are not supported with this method. In addition, as the number of devices increases, the polling thread can become resource intensive and CPU usage can significantly increase.

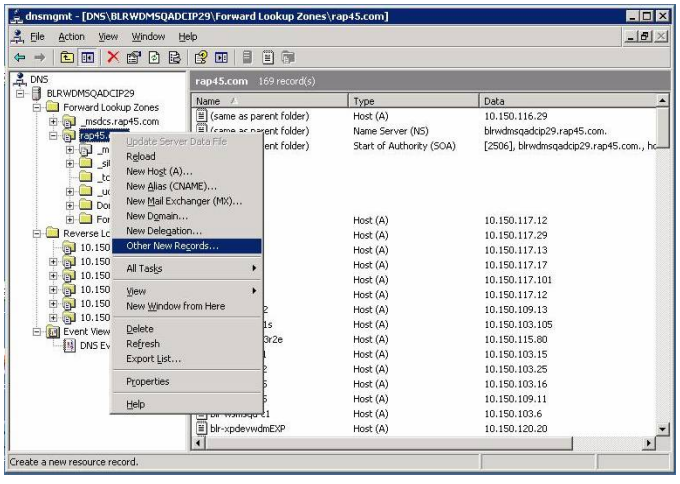
Creating a DNS Service Location (SRV) Resource Record for Wyse ThreadX Devices

If you plan to use Wyse ThreadX devices, you must create and configure a DNS Service Location (SRV) resource record.

Use the following guidelines:

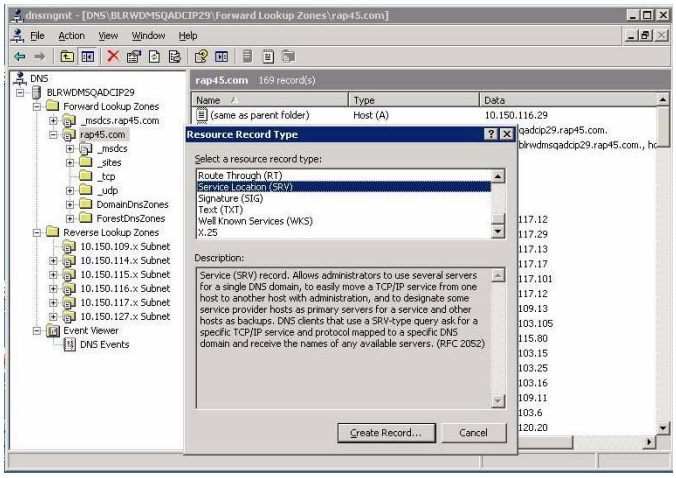
1. Open the DNS management console.

Figure 1 Other New Records



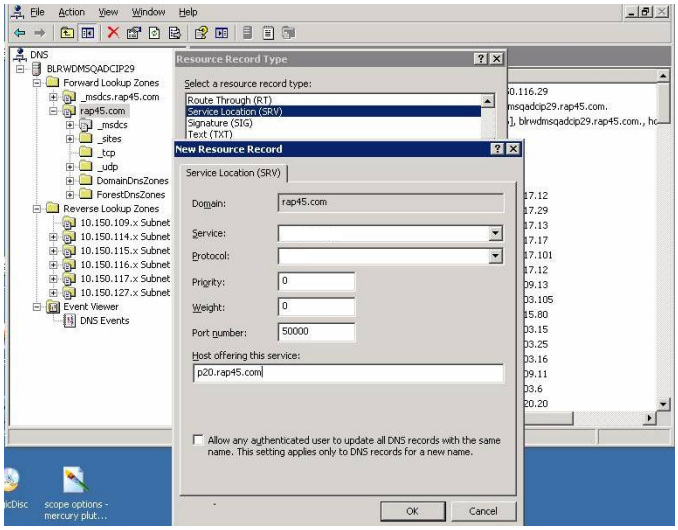
2. Select the domain where the server is configured, right-click it, and then select **Other New Records** to open the **Resource Record Type** dialog box.

Figure 2 Service Location (SRV)



3. Select the Service Location (SRV) resource record type and then click **Create Record** to open the **New Resource Record** dialog box.

Figure 3 New Resource Record



4. Use the following guidelines (**Domain** is automatically shown):

- Enter _**Pcoip-tool** in the *Service* box.
- Enter _**tcp** in the *Protocol* box.
- (Optional) Enter the value you want for this WDM server in the *Priority* box (the lower the priority value the higher the priority).
- (Optional) Enter the value you want for this WDM server in the *Weight* box (within the same priority class the higher the weight value the higher the priority).
- Enter **50000** in the *Port number* box.
- Enter the <FQDN of the WDM server> (for example, *p20.rap45.com*) in the *Host offering this service* box.

5. Click **OK**.

3 Installing or Upgrading WDM Workgroup Edition

This section provides the detailed procedures you must complete to install or upgrade *WDM Workgroup Edition*.

Caution

Be sure you have completed all pre-installation requirements as described in *"Preparing for Installation" before* you begin installing or upgrading *WDM Workgroup Edition*.

WDM Workgroup Edition installs the following WDM components on a single server:

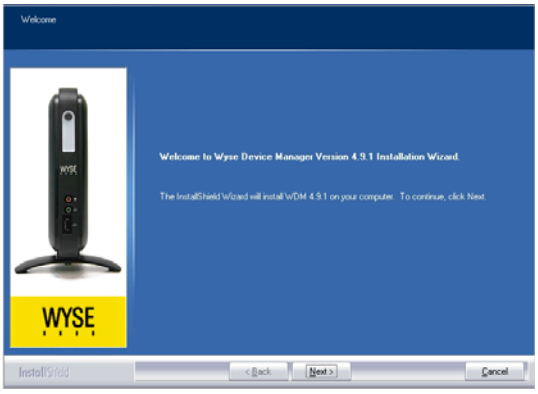
- WDM Database (**Database**) - Stores and provides access to all of the information for device management, including logging, packages, user data, and Remote Software Repository information.
- Software Repository (**Repository**) - Stores WDM packages for deployment use.
- Web Services (**HServer**) - Uses HTTP/HTTPS to enable push and pull communications to devices equipped with the WDM Web Agent.
- **Standard Services** - Allows WDM to:
  - Execute pre-boot management functions on devices that support Preboot Execution Environment (PXE).
  - Upgrade older WDM Web Agents to the latest WDM Web Agent.
- Administrator Console (**MMC Snap-in**) - User interface allows you to manage all of your network devices easily and quickly.

Installing or Upgrading Procedures (WDM Workgroup Edition)

The *WDM Workgroup Edition* installation wizard automatically detects whether a new installation or an upgrade installation is needed, and guides you through the process. Use the following guidelines:

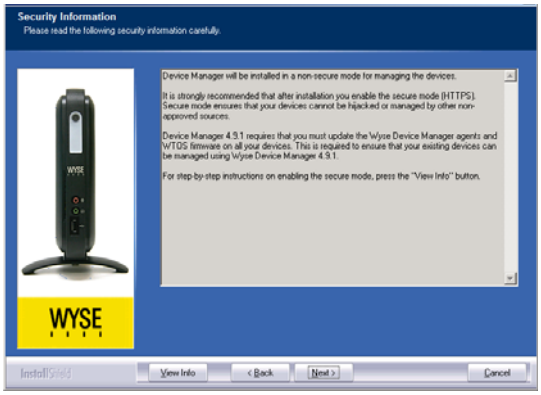
1. Download and extract the *WDM Workgroup Edition* files to a folder on the machine to which you will install WDM (for upgrades, this is the machine on which you are currently running *WDM Workgroup Edition version 4.9.0*).
2. Double-click **Setup.exe** to open and use the *InstallShield Wizard*.

Figure 4 InstallShield Wizard - Workgroup Edition

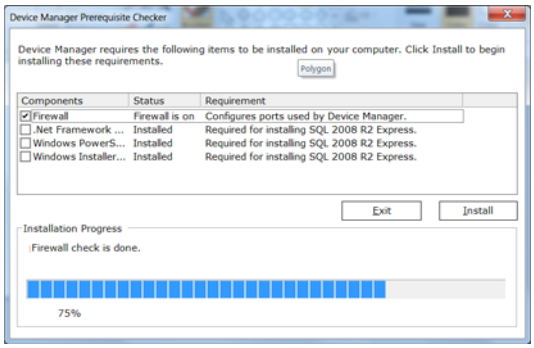

Welcome
Welcome to Wyse Device Manager Version 4.9.1 Installation Wizard.
The InstallShield Wizard will install WDM 4.9.1 on your computer. To continue, click Next.
WYSE
InstallShield
< Back
Next >
Cancel

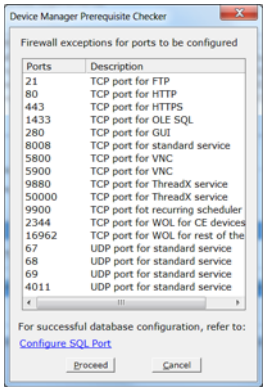
Use the following guidelines:

- **Be Sure to Use the WDM *Workgroup Sales Key*** - It appears by default in the *Customer Information* window of the *InstallShield Wizard*.
- **(Configuring Secure Communications) Be Sure to Carefully Follow the Security Information** - If you intend to configure secure communications, be sure to click the **View Info** button when the installation wizard displays information on secure communications. The information will help you to configure secure communications between the different components of WDM.

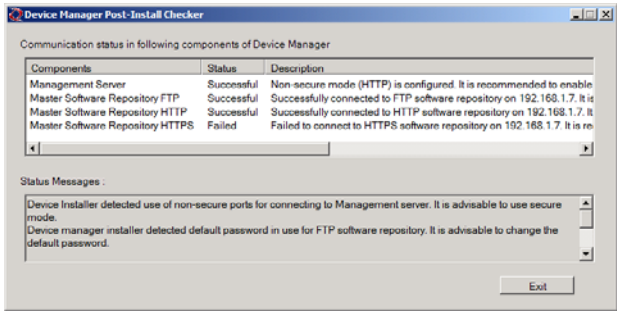

Security Information
Please read the following security information carefully.
Device Manager will be installed in a non-secure mode for managing the devices.
It is strongly recommended that after installation you enable the secure mode (HTTPS). Secure mode ensures that your devices cannot be hijacked or managed by other non-approved sources.
Device Manager 4.9.1 requires that you must update the Wyse Device Manager agents and WTOS firmware on all your devices. This is required to ensure that your existing devices can be managed using Wyse Device Manager 4.9.1.
For step-by-step instructions on enabling the secure mode, press the "View Info" button.
WYSE
InstallShield
View Info
< Back
Next >
Cancel

- **Be Sure to Carefully Follow the WDM Prerequisite Utility** - It finds out what you have and what you need, and then guides you through all the steps needed for your environment.




Device Manager Prerequisite Checker
Firewall exceptions for ports to be configured
Ports
Description
21 TCP port for FTP
80 TCP port for HTTP
443 TCP port for HTTPS
1433 TCP port for OLE SQL
280 TCP port for GUI
8008 TCP port for standard service
5800 TCP port for VNC
5900 TCP port for VNC
9880 TCP port for ThreadX service
50000 TCP port for ThreadX service
9900 TCP port fot recurring scheduler
2344 TCP port for WOL for CE devices
16962 TCP port for WOL for rest of the
67 UDP port for standard service
68 UDP port for standard service
69 UDP port for standard service
4011 UDP port for standard service
For successful database configuration, refer to:
Configure SQL Port
Proceed
Cancel

- **If You are Upgrading** - Be sure to use the correct system administrator password (*SA Password*) for the current installation of your *WDM Workgroup Edition*.
- **Use FTP for Repository Communication** - When selecting the protocol to use for repository communication be sure to use FTP (HTTP is not supported for *WDM Workgroup Edition* installations).
- **Be Sure to Carefully Follow the Post-Install Checker Recommendations** - The *WDM Post-Install Checker* displays component status and provides recommendations on matters such as security.


Device Manager Post-Install Checker
Communication status in following components of Device Manager
Components
Status
Description
Management Server
Successful
Non-secure mode (HTTP) is configured. It is recommended to enable
Master Software Repository FTP
Successful
Successfully connected to FTP software repository on 192.168.1.7. It is
Master Software Repository HTTP
Successful
Successfully connected to HTTP software repository on 192.168.1.7. It
Master Software Repository HTTPS
Failed
Failed to connect to HTTPS software repository on 192.168.1.7. It is re
Status Messages :
Device Installer detected use of non-secure ports for connecting to Management server. It is advisable to use secure mode.
Device manager installer detected default password in use for FTP software repository. It is advisable to change the default password.
Exit

- **Restart Your Computer after Installation is Complete** - Select the **Yes, I want to restart my computer now** option, remove any disks from their drives, and then click **Finish**.

3. After installing *WDM Workgroup Edition*, it is best practice to activate your WDM *Workgroup Sales Key* with an *Activation Code* at this time as described in "Activating Your Sales Key." **CAUTION**: Although you have 30 days in which to activate your WDM *Workgroup Sales Key* (after 30 days you cannot use WDM until you do activate it), it is highly recommended to do so at this time, as you must perform the activation on the server to which you installed the *Administrator Console* (**MMC Snap-in**).

This page intentionally blank.

4 Installing or Upgrading WDM Enterprise Edition

This section provides the detailed procedures you must complete to install or upgrade *WDM Enterprise Edition*.

Caution

Be sure you have completed all pre-installation requirements as described in *"Preparing for Installation" before* you begin installing or upgrading *WDM Enterprise Edition*.

WDM Enterprise Edition installs the following WDM components on a single server (*Typical* installation) or on multiple servers (*Custom* installation):

- WDM Database (**Database**) - Stores and provides access to all of the information for device management, including logging, packages, user data, and Remote Software Repository information (there can be only one instance of this WDM Database in your WDM environment).
- Software Repository (**Repository**) - Stores WDM packages for deployment use (in a *Custom* installation, you can have one Master Repository and multiple remote repositories in your WDM environment).
- Web Services (**HServer**) - Uses HTTP/HTTPS to enable push and pull communications to devices equipped with the WDM Web Agent (in a *Custom* installation, it is recommended to have as many instances of this Web Services as you have repository instances in your WDM environment).
- **Standard Services** - Allows WDM to (there can be only one instance of this Standard Services in your WDM environment):
  - Execute pre-boot management functions on devices that support Preboot Execution Environment (PXE).
  - Upgrade older WDM Web Agents to the latest WDM Web Agent.
- Administrator Console (**MMC Snap-in**) - User interface allows you to manage all of your network devices easily and quickly (in a *Custom* installation, you can have multiple instances of this Administrator Console in your WDM environment).

Tip

Using a WDM *Enterprise Sales Key* or *Enterprise Evaluation License Key* during installation allows the WDM components to be separately installed on different servers.

About Evaluation Licensing

If you are installing *WDM Enterprise Edition* for evaluation, you must use an *Enterprise Evaluation License Key* to install and use WDM for 30 days. To continue using WDM beyond 30 days without interruption, be sure to purchase and activate a WDM *Enterprise Sales Key* (as described in *Administrators Guide: Wyse Device Manager™*) *before* your 30 day evaluation period ends (after 30 days of evaluation, you cannot use WDM until you purchase and activate a WDM *Enterprise Sales Key*).

Installing or Upgrading Procedures (WDM Enterprise Edition)

The *WDM Enterprise Edition* installation wizard automatically detects whether a new installation or an upgrade installation from is needed, and guides you through the process (if you plan to install or upgrade WDM components on multiple machines using a *Custom* installation, you will repeat some of the installation procedures in this guide according to your environment design).

Use the following guidelines:

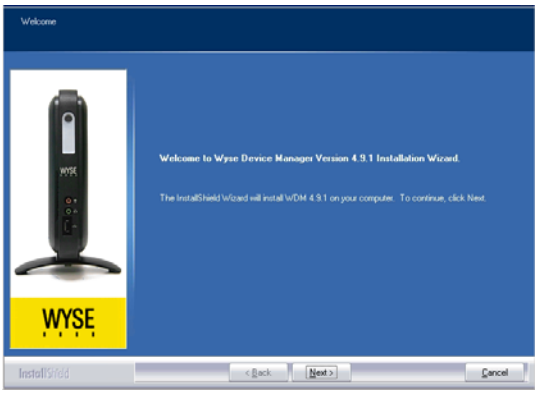
1. Download and extract the *WDM Workgroup Edition* files to a folder on the machine(s) to which you will install WDM (for upgrades, these are the machine(s) on which you are currently running *WDM Enterprise Edition version 4.9.0 components*).

Tip

The *WDM Workgroup Edition* files will automatically expand to a *WDM Enterprise Edition* installation/upgrade when you apply your WDM *Enterprise Sales Key* or *Enterprise Evaluation License Key* when prompted.

2. Double-click **Setup.exe** to open and use the *InstallShield Wizard*.

Figure 5 InstallShield Wizard - Enterprise Edition


Welcome
Welcome to Wyse Device Manager Version 4.9.1 Installation Wizard.
The InstallShield Wizard will install WDM 4.9.1 on your computer. To continue, click Next.
WYSE
InstallShield
< Back
Next >
Cancel

Use the following guidelines:

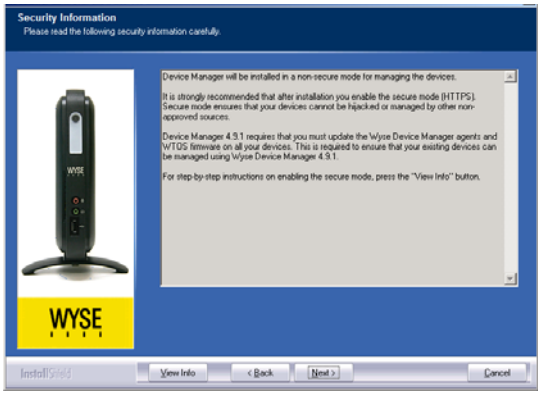
Tip

Use the Correct *Key* - For all WDM Enterprise Edition installations or upgrades (*Typical* or *Custom*) be sure to use the correct WDM *Enterprise Sales Key* or *Enterprise Evaluation License Key* provided to you by Wyse (after purchase, you should have received an email from Wyse or your reseller with full instructions on registering and generating your WDM *Enterprise Sales Key*; if you did not receive this email, contact your reseller).

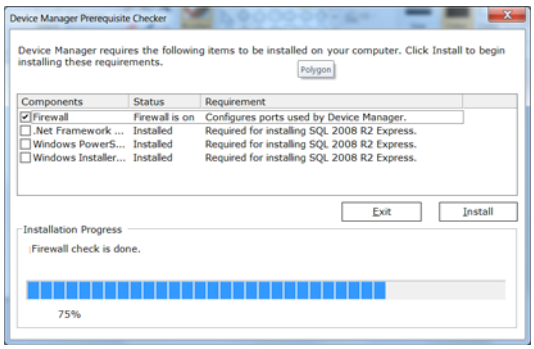
Caution

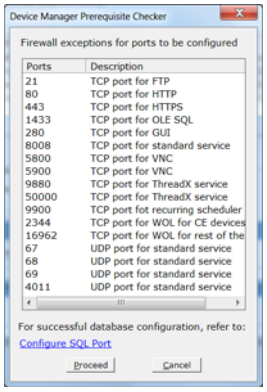
Do not use the WDM *Workgroup Sales Key* that appears by default in the *Customer Information* window of the *InstallShield Wizard*.

- **(Configuring Secure Communications) Be Sure to Carefully Follow the Security Information** - If you intend to configure secure communications, be sure to click the **View Info** button when the installation wizard displays information on secure communications. The information will help you to configure secure communications between the different components of WDM.

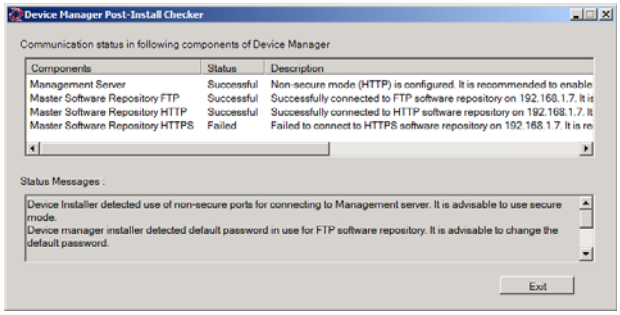

Security Information
Please read the following security information carefully.
Device Manager will be installed in a non-secure mode for managing the devices.
It is strongly recommended that after installation you enable the secure mode (HTTPS). Secure mode ensures that your devices cannot be hijacked or managed by other non-approved sources.
Device Manager 4.9.1 requires that you must update the Wyse Device Manager agents and WTOS firmware on all your devices. This is required to ensure that your existing devices can be managed using Wyse Device Manager 4.9.1.
For step-by-step instructions on enabling the secure mode, press the "View Info" button.
WYSE
InstallShield
View Info
< Back
Next >
Cancel

- **Be Sure to Carefully Follow the WDM Prerequisite Utility** - It finds out what you have and what you need, and then guides you through all the steps needed for your environment.




Device Manager Prerequisite Checker
Firewall exceptions for ports to be configured
Ports
Description
21 TCP port for FTP
80 TCP port for HTTP
443 TCP port for HTTPS
1433 TCP port for OLE SQL
280 TCP port for GUI
8008 TCP port for standard service
5800 TCP port for VNC
5900 TCP port for VNC
9880 TCP port for ThreadX service
50000 TCP port for ThreadX service
9900 TCP port fot recurring scheduler
2344 TCP port for WOL for CE devices
16962 TCP port for WOL for rest of the
67 UDP port for standard service
68 UDP port for standard service
69 UDP port for standard service
4011 UDP port for standard service
For successful database configuration, refer to:
Configure SQL Port
Proceed
Cancel

- **If You are Upgrading** - Be sure to use the correct system administrator password (*SA Password*) for the current installations of your *WDM Enterprise Edition*.
- **For *Typical* Installations and Upgrades, Use Defaults** - It is recommended to use the *InstallShield Wizard* recommendations.
  IMPORTANT: Typical installations are for FTP use only. If you want to use HTTP or HTTPS, you *must* perform a custom installation (see "Detailed Custom Installation and Upgrade Instructions").
- **For *Custom* Installations and Upgrades, Use the Detailed Instructions** - Use the detailed instructions in "Detailed Custom Installation and Upgrade Instructions."
- **Be Sure to Carefully Follow the Post-Install Checker Recommendations** - The *WDM Post-Install Checker* displays component status and provides recommendations on matters such as security.


Device Manager Post-Install Checker
Communication status in following components of Device Manager
Components
Status
Description
Management Server
Successful
Non-secure mode (HTTP) is configured. It is recommended to enable
Master Software Repository FTP
Successful
Successfully connected to FTP software repository on 192.168.1.7. It is
Master Software Repository HTTP
Successful
Successfully connected to HTTP software repository on 192.168.1.7. It
Master Software Repository HTTPS
Failed
Failed to connect to HTTPS software repository on 192.168.1.7. It is re
Status Messages :
Device Installer detected use of non-secure ports for connecting to Management server. It is advisable to use secure mode.
Device manager installer detected default password in use for FTP software repository. It is advisable to change the default password.
Exit

- **Restart Your Computer after Installation is Complete** - Select the **Yes, I want to restart my computer now** option, remove any disks from their drives, and then click **Finish**.

3. (*Installations on Windows Server 2008 Only*) - During the installation, if you are prompted to download and install the WebDAV Extension for IIS 7.0, simply follow the instructions (see also "Installing WebDAV Extension for IIS 7.0").
4. (Optional) *Using WDM Enterprise Sales Key Only* - After installing *WDM Enterprise Edition* and completing all of the required configurations for your WDM environment, it is best practice to activate your WDM *Enterprise Sales Key* with an *Activation Code* at this time as described in "Activating Your Sales Key."

Tip

Although you have 30 days in which to activate your *WDM Enterprise Sales Key* (after 30 days you cannot use WDM until you do activate it), it is highly recommended to do so at this time, as you must perform the activation on the server to which you installed the *Administrator Console* (**MMC Snap-in**).
CAUTION: A WDM *Enterprise Evaluation License Key* cannot be activated.

Detailed Custom Installation and Upgrade Instructions

Whether you are performing a *Custom* installation or upgrade on a single server or multiple servers, you must install or upgrade the WDM components in the following order:

1. WDM Database (**Database**) - There can be only one instance of this WDM Database in your WDM environment.
2. Software Repository (**Repository**) - You can have one Master Repository and multiple remote repositories in your WDM environment.
3. Web Services (**HServer**) - It is recommended to have as many instances of this Web Services as you have repository instances in your WDM environment.
4. **Standard Services** - There can be only one instance of this Standard Services in your WDM environment.
5. Administrator Console (**MMC Snap-in**) - You can have multiple instances of this Administrator Console in your WDM environment.

Depending on your installation selections, the installation wizard will automatically guide you through the *specific* process you need. When installing or upgrading each component grouping you want on a server, use the following tips (although upgrades do not show installation wizard screens, you can still use the information contained in these sections):

- "WDM Database Installation Tips You Need to Know"
- "Software Repository Installation Tips You Need to Know"
- "Administrator Console Installation Tips You Need to Know"

Tip

If you are installing or upgrading WDM components on multiple machines (requires repeating the installation wizard for each component grouping you want), be sure to select the correct components for the server on which you are installing or upgrading components. For example, you can use the *InstallShield Wizard* to install the WDM *Database* on one server, and then use the *InstallShield Wizard* to install the other components on a second server. Your WDM *Enterprise Sales Key* allows the WDM components to be separately installed on different servers.

Caution

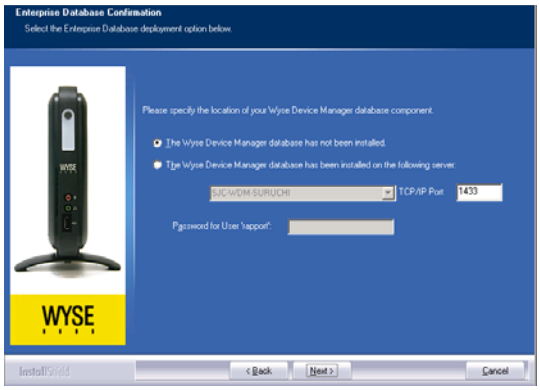
(*Installations on Windows Server 2008 Only*) - During the installation, if you are prompted to download and install the WebDAV Extension for IIS 7.0, simply follow the instructions (see also "Installing WebDAV Extension for IIS 7.0").

WDM Database Installation Tips You Need to Know

Depending on *how* you are installing, use the following guidelines when prompted for *Database* configurations during an installation or upgrade:

- **If you are installing a new WDM *Database* on a server** - be sure to select the *The Wyse Device Manager database has not been installed* option.

Figure 6 Initial WDM Database installation

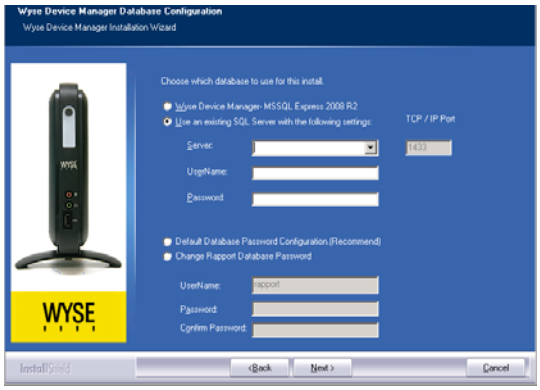

Enterprise Database Confirmation
Select the Enterprise Database deployment option below.
Please specify the location of your Wyse Device Manager database component.
The Wyse Device Manager database has not been installed.
The Wyse Device Manager database has been installed on the following server:
SJC-WDM-SURUCHI
TCP/IP Port
1433
Password for User 'rapport':
WYSE
InstallShield
< Back
Next >
Cancel

- **If you are using an existing SQL Server during your initial WDM *Database* installation configurations** - be sure to note the *Server* name, the *TCP/IP Port*, and the *Database Password* (for the default user named *rapport*), as you will use this information when you install the other WDM components. If you do not specify the TCP/IP Port for the WDM *Database*, the default **1433** is used (this is the port the database server uses for communication with WDM components).

Caution

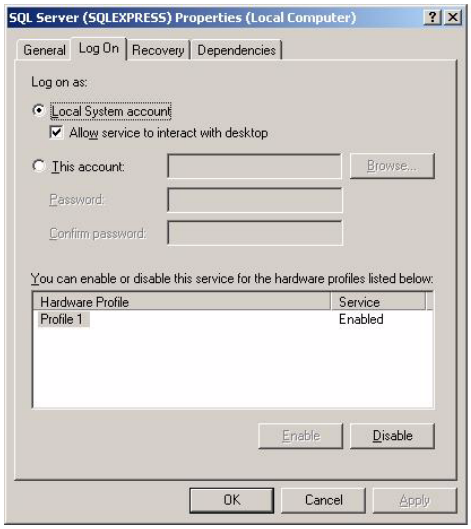
If you use the **Change Rapport Database Password** option (for example, to satisfy company password requirements), be sure to note the password for WDM installation use and general password recovery.

Figure 7 Database configuration



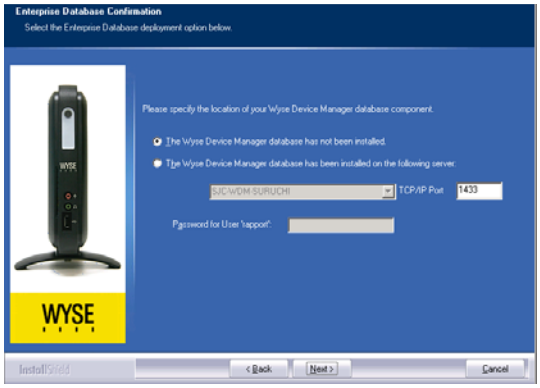
- **If you intend to use your *existing SQL Server 2005 Express Edition* for the WDM Database** - ensure the *Log on as* account for the *SQLExpress* service is set to *Local System account* as follows:
  From the **Start** menu on your server, navigate to **Administrative Tools > Services**, right-click **SQL Server (SQLEXPRESS) Service**, select **Properties**, click the **Log On** tab, select the *Local System account* option, select the **Allow service to interact with desktop** check box, click **OK**, and then restart the *SQL Server (SQLEXPRESS)* service.

Figure 8 SQL Server Properties



- **If you have already installed the WDM *Database* on a separate server and you are currently installing other WDM components on a server** - the *InstallShield Wizard* will prompt you for a WDM *Database* confirmation. Be sure to select the correct server name, enter the correct TCP/IP Port, and enter the correct database password (for the default user named *rapport*). These are the fields you entered during your WDM *Database* installation. If you do not specify the TCP/IP Port for the WDM *Database*, the default **1433** is used (this is the port the database server uses for communication with WDM components).

Figure 9 Database confirmation


Enterprise Database Confirmation
Select the Enterprise Database deployment option below.
Please specify the location of your Wyse Device Manager database component.
The Wyse Device Manager database has not been installed.
The Wyse Device Manager database has been installed on the following server:
SJC-WDM-SURUCHI
TCP/IP Port
1433
Password for User 'rapport':
WYSE
InstallShield
< Back
Next >
Cancel

- **If you have an existing SQL Server that was installed using *Windows Authentication mode* only** - WDM utilizes *mixed mode authentication*. Be aware that if you are using an existing SQL Server that was installed using *Windows Authentication mode* only, the WDM *Database* user will be unable to log in to the SQL database, and the WDM *Database* installation will fail. Therefore, you must open your SQL Server Configuration Manager and enable TCP/IP connections (see the Microsoft documentation for your SQL Server).

Software Repository Installation Tips You Need to Know

Depending on *how* you are installing, use the following guidelines when prompted for *Repository* configurations during an installation or upgrade:

Tip

If your network has multiple subnets, consider deploying a copy of the WDM *Software Repository* (**Repository**) on each subnet to allow you to store large device applications and image files locally. When upgrades are distributed to devices on a subnet from a local repository, network traffic is reduced.

- **When selecting the protocol to use for repository communication** - use the following guidelines (Note that the wizard attempts to connect to your FTP service to ensure connectivity and read/write permissions; WDM only verifies an existing connection; it does not configure your FTP service.):
  - **FTP** - Select this option if you want WDM to download packages from the repository using the FTP protocol. **CAUTION:** If you intend to use the firmware upgrade feature for Wyse ThreadX devices, FTP must be configured.
    If you are using an existing *FTP service*, the wizard prompts you for an IP Address, username, and password.
    If you are using an existing *IIS FTP service*, the wizard creates a local WDM user and assigns the user read/write permissions to the IIS FTP service.
  - **HTTP** - Select this option if you want WDM to download packages from the repository using the HTTP protocol.
  - **FTP and HTTP** - Select both options if you want WDM to download packages from the repository using *either* the FTP or HTTP protocol. If both options are selected, HTTP is attempted first; if HTTP fails, the FTP protocol is then attempted.

Tip

HTTPS (recommended) can be enabled/configured later on an HTTP repository. For information on configuring WDM to securely manage your Wyse cloud clients and zero clients (with general guidance and specific instructions on configuring WDM and Wyse devices for secure management), refer to Wyse Knowledge Base Solution **#22428** (go to the Wyse Knowledge Base at http://www.wyse.com/kb and search for **22428**).

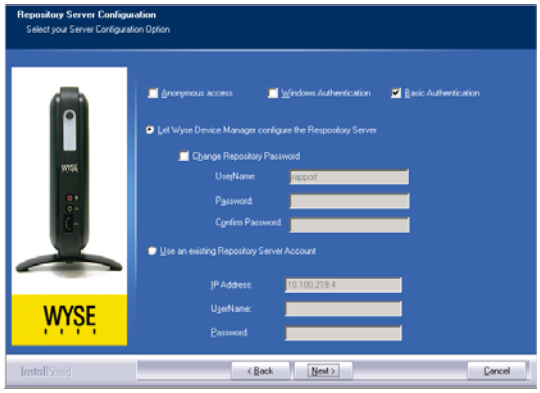
Figure 10 Repository communication protocol

Repository Server Configuration
Select your Server Configuration Option
Please select the Repository Protocol method
FTP Protocol
HTTP Protocol
Caution: FTP Protocol must be selected for ThreadXMgr to function.
Note : By selecting only http protocol rolling back to ftp protocol in the future may require user to manually copy the repository files.
It is recommended to Select both ftp and http protocol.
WYSE
InstallShield
< Back
Next >
Cancel

- **When selecting the authentication option(s) to apply to software repositories** - use the following guidelines (note that you can select any or all of the options; if you select all three options, *Windows Authentication* is applied.):
  - **Anonymous Access** - (*Not Recommended*) This mode does not require a username or password to access the repository.

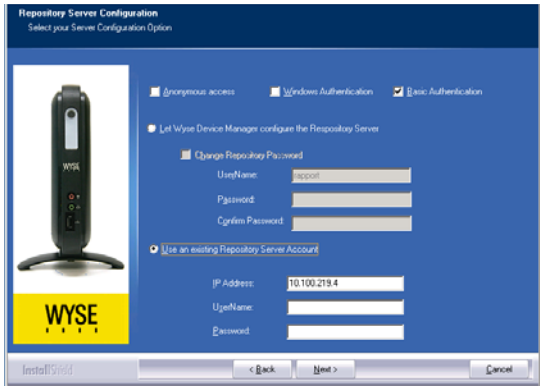
- **Windows Authentication** - This is the most secure form of authentication in IIS. When you log in, Windows NT validates your login and only your username is transmitted over the network. Your password is not transmitted.
- **Basic Authentication** - This authentication mode requires you to log in with a valid Windows NT username and password to access the system. The password is transmitted over the network in clear text.

Figure 11 Repository Authentication



- **If you have an existing repository server account instead of the default user account named *rapport*** - (for example, you are upgrading an existing WDM repository server or want to use an existing *Active Directory*) select the **Use an existing Repository Server Account** option, and then enter the *IP Address* (or server name) and the *UserName* and *Password* of that account.

Figure 12 Existing repository server account



Administrator Console Installation Tips You Need to Know

If you are installing multiple instances of the Administrator Console (**MMC Snap-in**) in your WDM environment and want to use other administrators for additional Administrator Console installations, you must do the following (in the order presented):

Caution

These instructions do not pertain to the *initial* installation of the Administrator Console for the local administrator.

1. Add the user (you want as the eventual administrator of the Administrator Console instance) using the *Configuration Manager* as described in *Administrators Guide: Wyse Device Manager™*.
2. Install the instance of the Administrator Console (**MMC Snap-in**) as described in "Installing or Upgrading Procedures (WDM Enterprise Edition)." Note that after this installation, the Administrator Console will not be able to connect to the WDM Database or a software repository in your WDM environment until you complete step 3.
3. After installing the instance of the Administrator Console, use the *Configuration Manager* (as described in *Administrators Guide: Wyse Device Manager™*) to edit the user you want as the administrator (from step 1) so that the user has administrator rights for that instance of the Administrator Console.

A Activating Your Sales Key

This appendix includes the detailed steps you must complete to activate your *Sales Key* (WDM *Workgroup Sales Key* or WDM *Enterprise Sales Key*).

Tip

A WDM *Enterprise Evaluation License Key* cannot be activated.

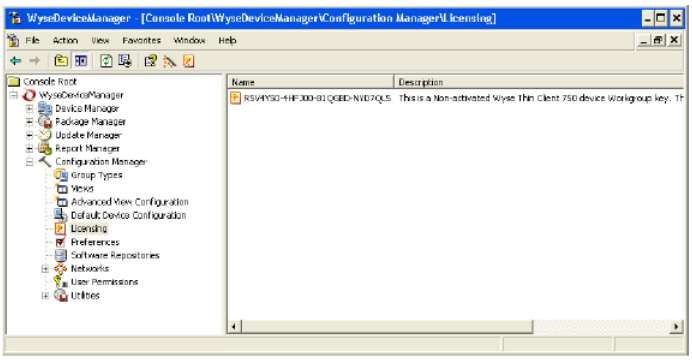
Caution

Be sure to perform the activation (enter an *Activation Code*) on the server to which you installed the *Administrator Console* (**MMC Snap-in**).

Use the following guidelines:

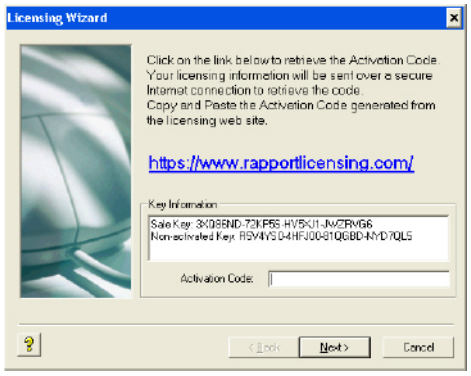
1. On the desktop of the server on which you installed the *Administrator Console* (**MMC Snap-in**), double-click the **WDM** icon to open the WDM *Administrator Console*.
2. In the tree pane, expand **Configuration Manager** and select **Licensing** to show the *Non-activated* WDM *Sales Key* in the details pane.

Figure 13 WDM Administrator Console - Licensing



3. Right-click the *Non-activated* WDM *Sales Key* and select **Activate** to open the *Licensing Wizard*.

Figure 14 Licensing Wizard


Licensing Wizard
Click on the link below to retrieve the Activation Code.
Your licensing information will be sent over a secure Internet connection to retrieve the code.
Copy and Paste the Activation Code generated from the licensing web site.
https://www.rapportlicensing.com/
Key Information
Activation Code:
< Back
Next >
Cancel

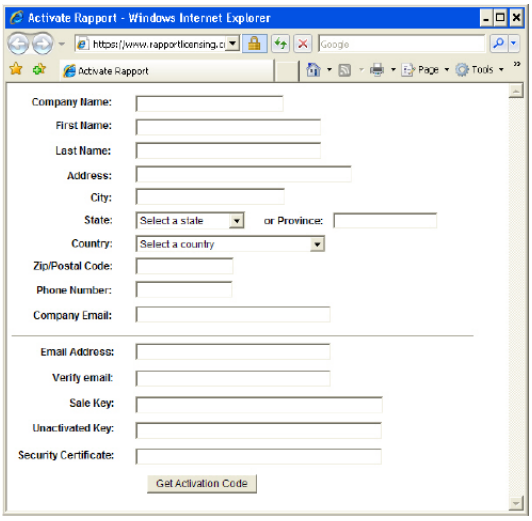
4. Note your *Sales Key* and *Non-activated Key* numbers as you will use them in the online WDM licensing form.

Tip

If the server on which you installed the *Administrator Console* (**MMC Snap-in**) has internet access, you can copy-and-paste the *Sales Key* and *Non-activated Key* numbers from the *Key Information* area of the *Licensing Wizard* into the online WDM licensing form.

5. On a server which has internet access, use your browser to open the online WDM licensing form at: https://www.rapportlicensing.com/clientframe/rapport.aspx.

Figure 15 Licensing form



6. Enter the information to complete the form (be sure to use the correct *Sales Key* and *Non-activated Key* numbers, and enter uppercase **B** for *Security Certificate*).

7. After completing the form, click **Get Activation Code** to display the *Activation Code* (an e-mail containing the *Activation Code* is also sent to the *Email Address* you provided).

8. In the *Licensing Wizard* on the server to which you installed the *Administrator Console* (**MMC Snap-in**), enter (or copy-and-paste) the *Activation Code* into the **Activation Code** box, and then click **Next** to open the details pane displaying your *Sales Key* as *Activated*.

B Uninstalling WDM

When using a Microsoft Windows remove program feature (such as *Add and Remove Programs* or *Programs and Features*) to remove WDM, the database server will require login credentials to complete the uninstallation of WDM.

Figure 16 Database Server Login Credentials

Database Server Login
Database server requires login credentials to continue.
Specify SQL Login ID and Password for SQL Server.
Specify SQL Login ID and WDM Database Password for MSDE and SQL Express.
Login ID:
Password:
WYSE
InstallShield
< Back
Next >
Cancel

Depending on your WDM installation, do one of the following:

- *WDM Workgroup Edition* - You must enter **sa** for the *Login ID* and enter **ThinMgmt_451** for the *Password*.
- *WDM Enterprise Edition* - Depending on your WDM installation, do one of the following:
  - If you had WDM install the default Microsoft SQL Server 2008 R2 Express (32-bit) as your database server, enter **sa** for the *Login ID* and enter **ThinMgmt_451** for the *Password*.
  - If you used an *existing* database server during your WDM installation (that is, any supported database server that is *not installed* by WDM during the WDM installation - see "Software Requirements" and "WDM Database Installation Tips You Need to Know"), enter **sa** for the *Login ID* and your *Password* for that server.

At the end of the uninstalling process, the wizard will prompt you to restart. Select the **Yes, I want to restart my computer now** option and click **Finish**.

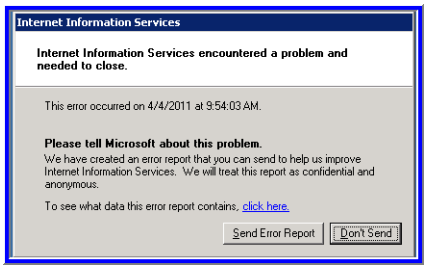
Caution

If you see Microsoft data execution prevention and IIS error messages after server restart, you must complete these additional steps to remove the **RapportFilter** entry from IIS manually.

Figure 17 Microsoft data execution prevention message - example

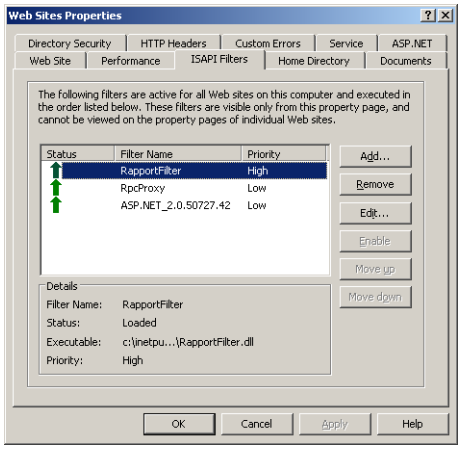
Data Execution Prevention - Microsoft Windows
To help protect your computer, Windows has closed this program.
Name: Internet Information Services
Publisher: Microsoft Corporation
Change Settings
Close Message
Data Execution Prevention helps protect against damage from viruses or other threats. Some programs might not run correctly when it is turned on. For an updated version of this program, contact the publisher. What else should I do?

Figure 18 IIS error message - example


Internet Information Services
Internet Information Services encountered a problem and needed to close.
This error occurred on 4/4/2011 at 9:54:03 AM.
Please tell Microsoft about this problem.
We have created an error report that you can send to help us improve Internet Information Services. We will treat this report as confidential and anonymous.
To see what data this error report contains, click here.
Send Error Report
Don't Send

Open the **IIS Web Sites Properties** dialog box (according to the IIS documentation for your server version).

Figure 19 Remove the RapportFilter entry from IIS - example



On the *ISAPI Filters* tab, select **RapportFilter** from the list, click **Remove**, confirm, and then click **OK**.

After removing the **RapportFilter** entry from IIS, restart the server. You should no longer see Microsoft data execution prevention and IIS error messages after server restart.

C Reference and Troubleshooting: FTP, IIS, and Firewall Information

Although WDM automatically installs and configures everything you need for WDM use with respect to FTP, IIS, and the Windows Firewall, the following reference information can be useful for understanding your environment and for various troubleshooting purposes.

Information includes:

- "How the WDM Installer Installs and Configures FTP"
- "How the WDM Installer Installs and Configures IIS"
- "Using Windows Firewall with WDM"

How the WDM Installer Installs and Configures FTP

Depending on your server version, use one of the following sections to understand how FTP is installed and configured for use with WDM (information is presented as if you would complete the procedures manually):

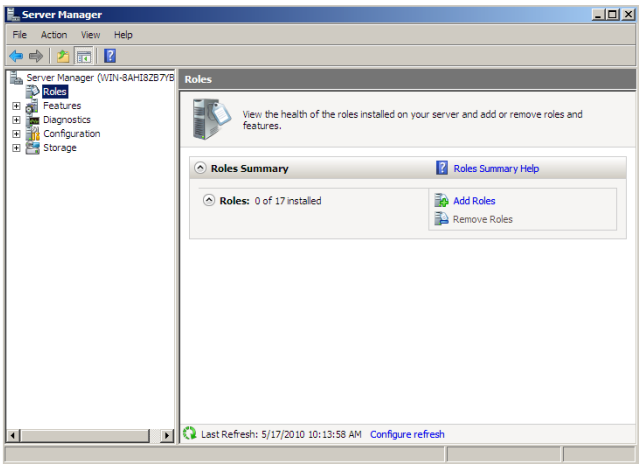
- "Installing and Configuring FTP on Windows Server 2008"
- "Installing and Configuring FTP on Windows Server 2008 R2"
- "Installing and Configuring FTP on Windows 7"

Installing and Configuring FTP on Windows Server 2008

Before setting up your own FTP server in Windows, you must be sure that Internet Information Services (IIS) has already been installed on the server.

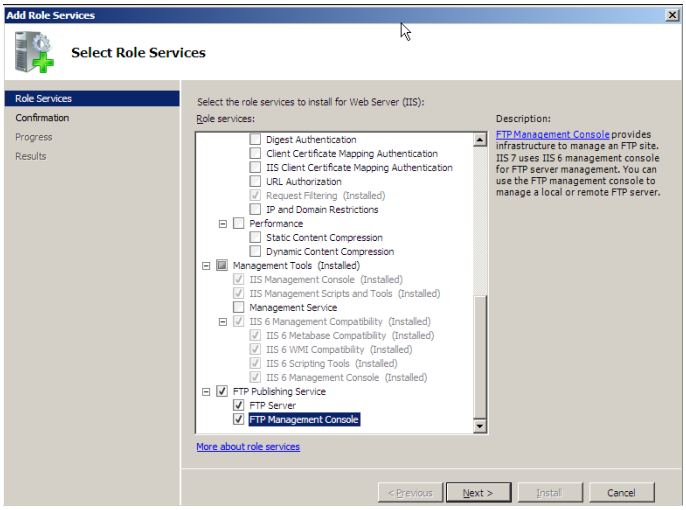
1. On the taskbar, click **Start > Administrative Tools > Server Manager** to open the **Server Manager window**.

Figure 20 Server Manager



2. In the *Server Manager* tree pane, expand **Roles**, and then click **Web Server (IIS)** to open the **Web Server (IIS)** window.
3. In the details pane of the **Web Server (IIS)** window, scroll to **Role Services**, and then click **Add Role Services** to open the **Select Role Services** window.

Figure 21 Select Role Services

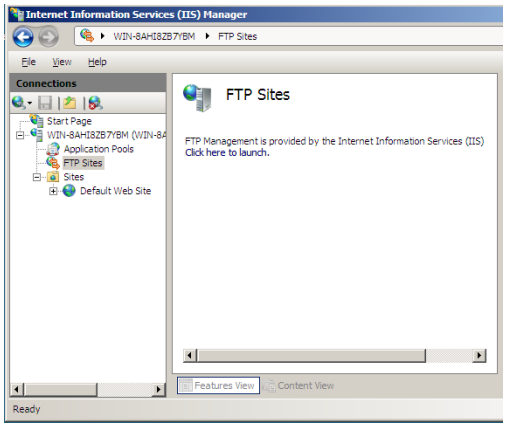

Add Role Services
Select Role Services
Role Services
Confirmation
Progress
Results
Select the role services to install for Web Server (IIS):
Role services:
Digest Authentication
Client Certificate Mapping Authentication
IIS Client Certificate Mapping Authentication
URL Authorization
Request Filtering (Installed)
IP and Domain Restrictions
Performance
Static Content Compression
Dynamic Content Compression
Management Tools (Installed)
IIS Management Console (Installed)
IIS Management Scripts and Tools (Installed)
Management Service
IIS 6 Management Compatibility (Installed)
IIS 6 Metabase Compatibility (Installed)
IIS 6 WMI Compatibility (Installed)
IIS 6 Scripting Tools (Installed)
IIS 6 Management Console (Installed)
FTP Publishing Service
FTP Server
FTP Management Console
Description:
FTP Management Console provides infrastructure to manage an FTP site. IIS 7 uses IIS 6 management console for FTP server management. You can use the FTP management console to manage a local or remote FTP server.
More about role services
< Previous
Next >
Install
Cancel

4. Under **Role Services**, expand **FTP Publishing Service**, select the **FTP Server** and **FTP Management Console** check boxes, and then click **Next** to open the **Confirm Installation Selections** window.
5. After confirming, click **Install**.
6. After installation is complete (the **Results** window displays a successful installation), click **Close**.

Use the following guidelines to configure FTP on Windows Server 2008:

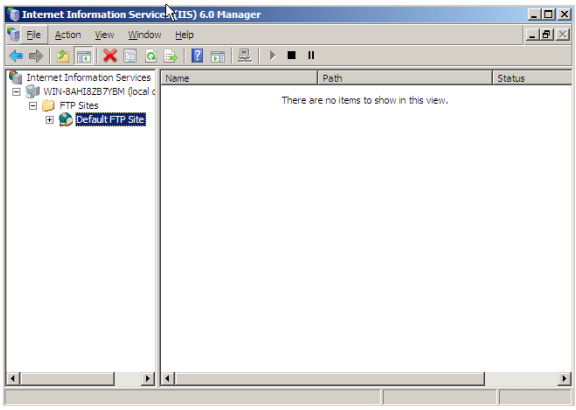
1. On the taskbar, click **Start > Administrative Tools > Internet Information Services (IIS) Manager** to open the **Internet Information Services (IIS) Manager** window.
2. In the tree pane, expand *Server_name* (where Server_name is the name of the server), and then select **FTP Sites**.

Figure 22 FTP Sites



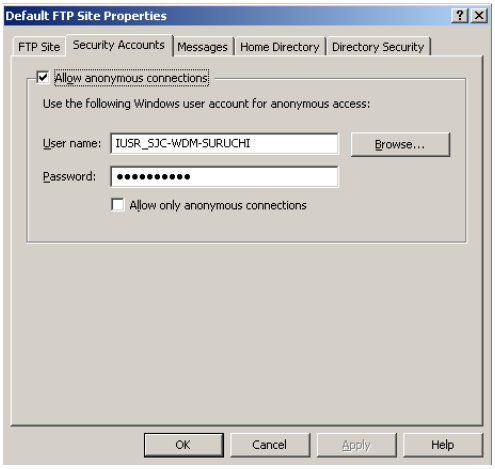
3. In the *FTP sites* details pane, click the **Click here to launch** link, to open the **IIS 6.0 Manager** window.
4. In the tree pane expand *Server_name* (where Server_name is the name of the server), and then expand **FTP Sites**.
   Note: If **FTP Site** is stopped, click on the start icon to start it.

Figure 23 Default FTP Site



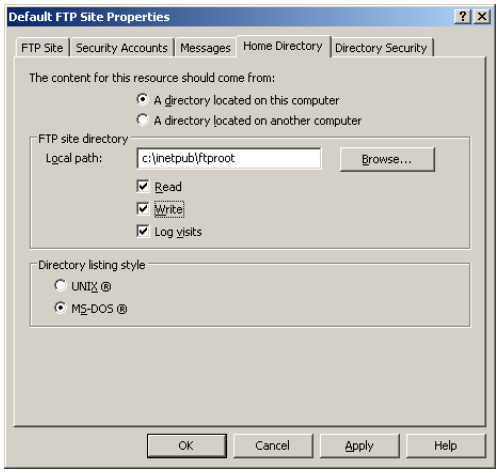
5. In the tree pane, right-click on **Default FTP Site**, and then select **Properties** to open the **Properties** dialog box.

Figure 24 Properties



6. Click the **Security Accounts** tab and be sure that the **Allow Anonymous Connections** check box is selected.

Figure 25 Home Directory tab



7. Click the **Home Directory** tab and be sure that the **Read**, **Write** and **Log visits** check boxes are selected.
8. Click **Apply**, and then click **OK**.
9. Close the **Internet Information Services (IIS) Manager** window.
10. The FTP server is now configured to accept incoming FTP requests. Copy or move the files that you want to make available to the FTP publishing folder for access. The default folder is *drive:**Inetpub**ftproot* (where drive is the drive on which IIS is installed).

Use the following guidelines to verify FTP on Windows Server 2008:

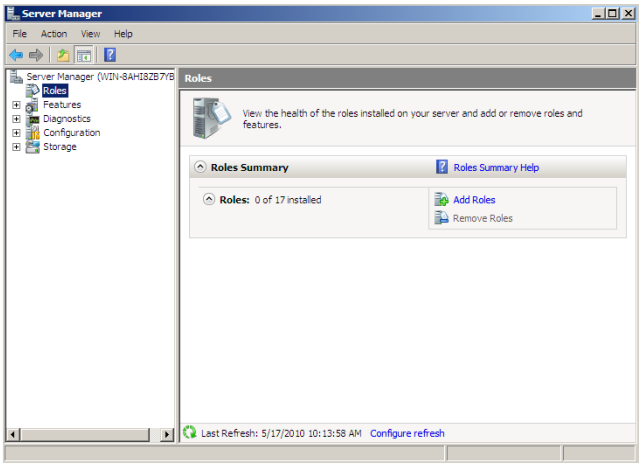
1. Open a command prompt (click **Start > Run**, enter **cmd**, and then click **OK**).
2. Type **ftp localhost**.
3. Enter an administrator user name and password.
4. Ensure that login is successful.
5. Open the services panel and make sure that the FTP service is configured to start automatically.

Installing and Configuring FTP on Windows Server 2008 R2

Before setting up your own FTP server in Windows, you must be sure that Internet Information Services (IIS) has already been installed on the server.

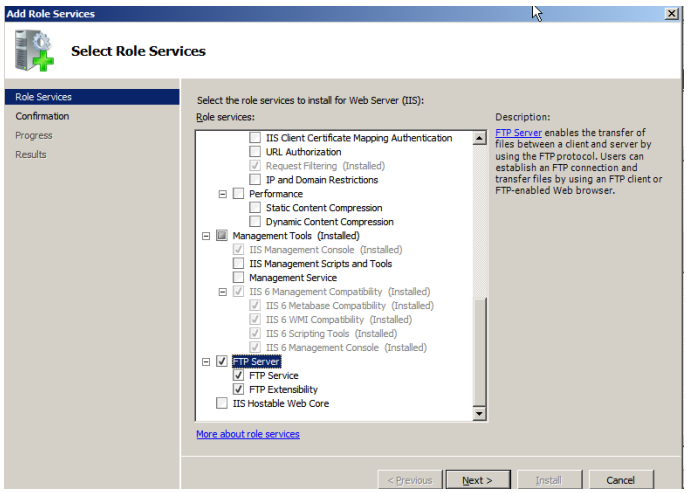
1. On the taskbar, click **Start > Administrative Tools > Server Manager** to open the **Server Manager** window.
2. In the *Server Manager* tree pane, expand **Roles**, and then click **Web Server (IIS)** to open the **Web Server (IIS)** window.

Figure 26 Web Server (IIS)



3. In the details pane of *Web Server (IIS)*, scroll to **Role Services**, and then click **Add Role Services** to open the **Select Role Services** window.

Figure 27 Select Role Services

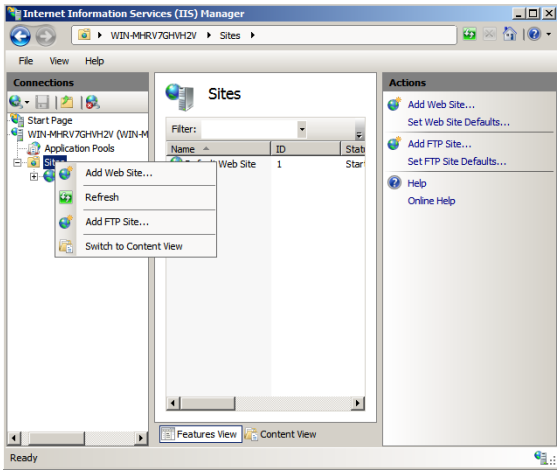

Add Role Services
Select Role Services
Role Services
Confirmation
Progress
Results
Select the role services to install for Web Server (IIS):
Role services:
IIS Client Certificate Mapping Authentication
URL Authorization
Request Filtering (Installed)
IP and Domain Restrictions
Performance
Static Content Compression
Dynamic Content Compression
Management Tools (Installed)
IIS Management Console (Installed)
IIS Management Scripts and Tools
Management Service
IIS 6 Management Compatibility (Installed)
IIS 6 Metabase Compatibility (Installed)
IIS 6 WMI Compatibility (Installed)
IIS 6 Scripting Tools (Installed)
IIS 6 Management Console (Installed)
FTP Server
FTP Service
FTP Extensibility
IIS Hostable Web Core
Description:
FTP Server enables the transfer of files between a client and server by using the FTP protocol. Users can establish an FTP connection and transfer files by using an FTP client or FTP-enabled Web browser.
More about role services
< Previous
Next >
Install
Cancel

4. Under **Role Services**, expand **FTP Server,** select the **FTP Service** and **FTP Extensibility** check boxes, and then click **Next** to open the **Confirm Installation Selections** window.
5. After confirming, click **Install**.
6. After installation is complete (the **Results** window displays a successful installation), click **Close.**

Use the following guidelines to configure FTP on Windows Server 2008 R2:

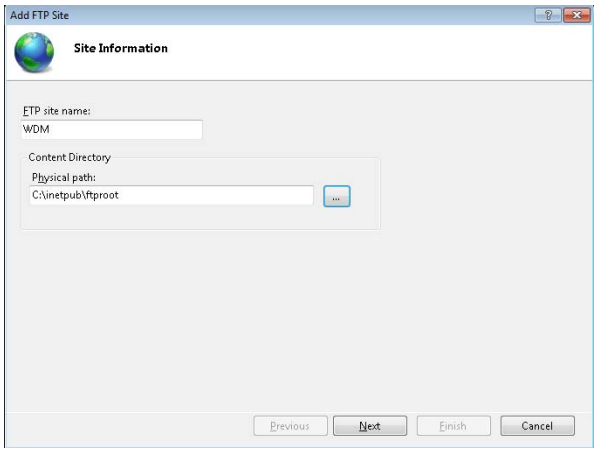
1. On the taskbar, click **Start > Administrative Tools > Internet Information Services (IIS) Manager** to open the **Internet Information Services (IIS) Manager** window.

Figure 28 Internet Information Services (IIS) Manager



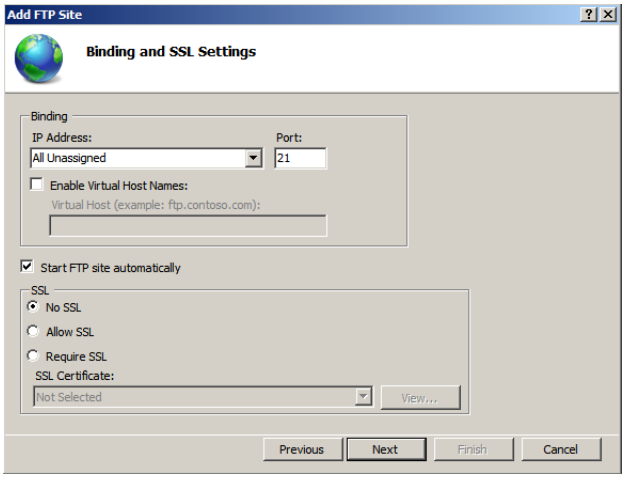
2. In the tree pane, right-click on **Sites**, and then select **Add FTP Site** to begin creating an FTP site.

Figure 29 Site Information



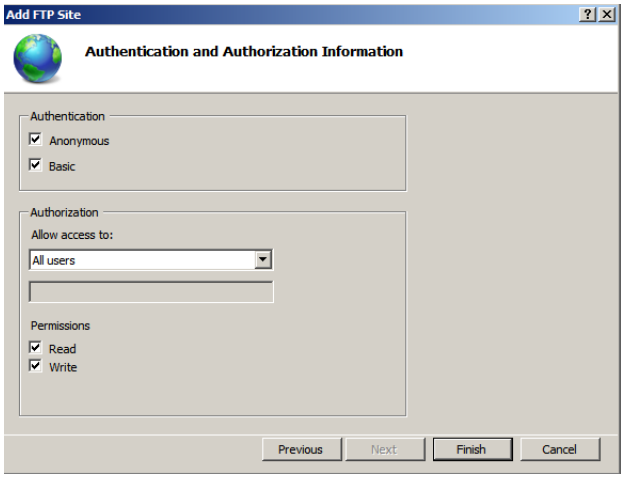
3. Enter the *FTP site name*, select the *Physical path* for the FTP root directory, and then click **Next**.

Figure 30 Binding and SSL Settings



4. Keep the default value for *IP Address* as **All unassigned** and port as **21**.
5. Select the **Start FTP site automatically** check box, change the *SSL* option to **No SSL**, and then click **Next**.

Figure 31 Authentication and Authorization Information



6. Select the **Anonymous** and **Basic Authentication** check boxes.
7. Select **All users** in the *Allow access to* list.
8. Select the **Read** and **Write** check boxes.
9. Click **Finish**.

Use the following guidelines to verify FTP on Windows Server 2008 R2:

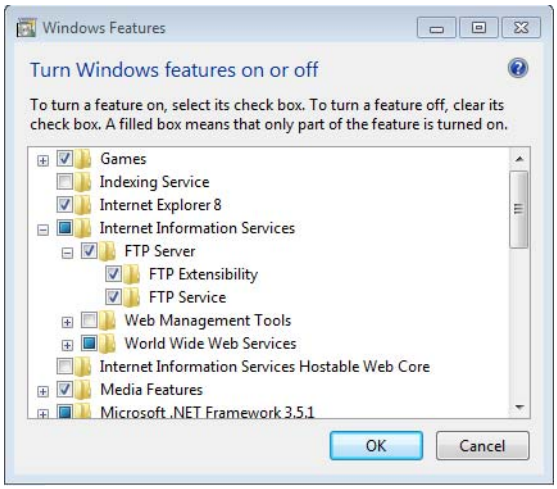
1. Open a command prompt (click **Start > Run**, enter **cmd**, and then click **OK**).
2. Type **ftp localhost**.
3. Enter an administrator user name and password.
4. Ensure that login is successful.

Installing and Configuring FTP on Windows 7

Before setting up your own FTP server in Windows, you must be sure that Internet Information Services (IIS) has already been installed on the server.

1. On the taskbar, click **Start > Control Panel** to open **Control Panel**.
2. Click **Programs > Programs and Features**, and then on the left pane click **Turn Windows Features on or off** to open the **Windows Features** window.
3. Scroll to **Internet Information Services**.

Figure 32 Internet Information Services

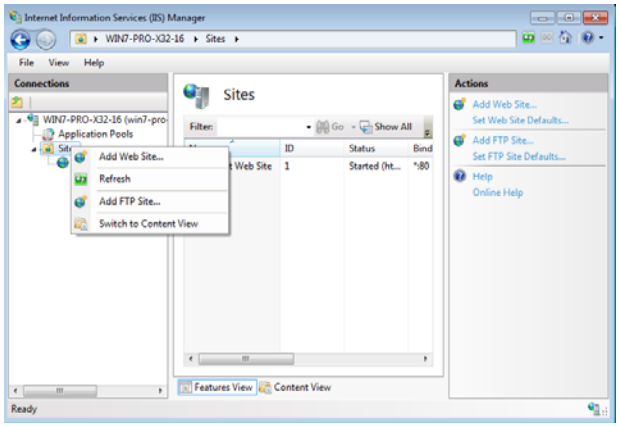

Windows Features
Turn Windows features on or off
To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.
Games
Indexing Service
Internet Explorer 8
Internet Information Services
FTP Server
FTP Extensibility
FTP Service
Web Management Tools
World Wide Web Services
Internet Information Services Hostable Web Core
Media Features
Microsoft .NET Framework 3.5.1
OK
Cancel

4. Expand **Internet Information Services,** and then expand **FTP Server**.
5. Under **FTP Server,** select the **FTP Extensibility** and **FTP Service** check boxes, and then click **OK** to install FTP.

Use the following guidelines to configure FTP on Windows 7:

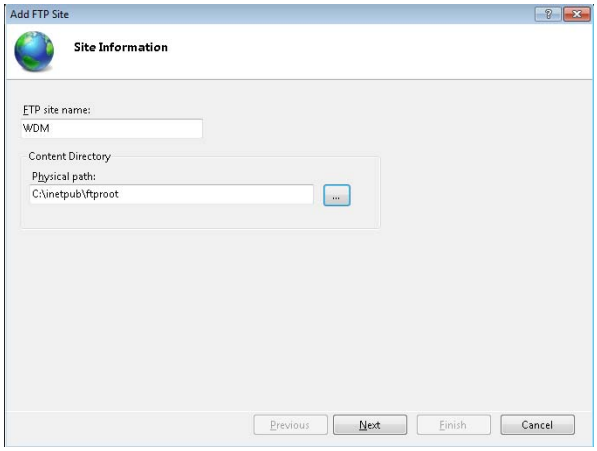
1. On the taskbar, click **Start > Control Panel > Administrative Tools > Internet Information Services (IIS) Manager** to open the *Internet Information Services (IIS) Manager*.
   Note: If you do not see **Administrative Tools** on *Control Panel*, select **Small icons** or **Large icons** in the *View by* list.

Figure 33 Internet Information Services (IIS) Manager



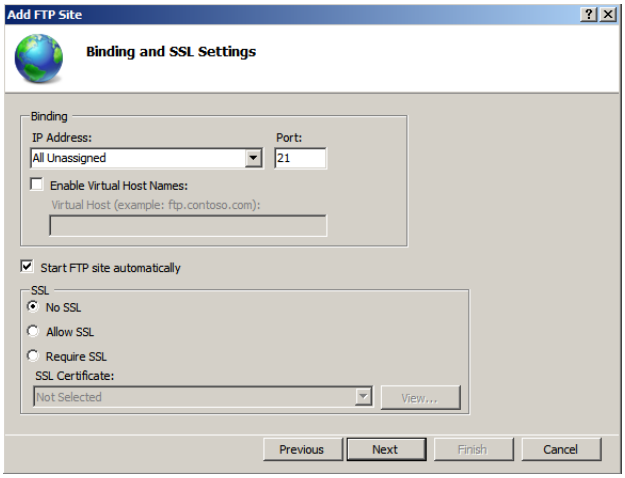
2. In the tree pane, right-click on **Sites**, and then select **Add FTP Site** to begin creating an FTP site.

Figure 34 Add FTP Site



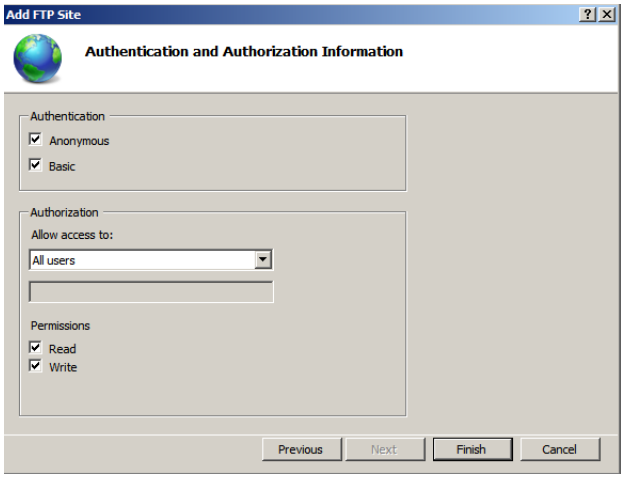
3. Enter the *FTP site name*, select the *Physical path* for the FTP root directory, and then click **Next**.

Figure 35 Binding and SSL Settings



4. Keep the default value for *IP Address* as **All unassigned** and port as **21**.
5. Select the **Start FTP site automatically** check box, change the *SSL* option to **No SSL**, and then click **Next**.

Figure 36 Authentication and Authorization Information



6. Select the **Anonymous** and **Basic Authentication** check boxes.
7. Select **All users** in the ***Allow access to*** list.
8. Select the **Read** and **Write** check boxes.
9. Click **Finish**.

Use the following guidelines to verify FTP on Windows 7:

1. Open a command prompt (click **Start > Run**, enter **cmd**, and then click **OK**).
2. Type **ftp localhost**.
3. Enter an administrator user name and password.
4. Ensure that login is successful.

How the WDM Installer Installs and Configures IIS

Depending on your operating system, use one of the following sections to understand how IIS is installed and configured for use with WDM (information is presented as if you would complete the procedures manually):

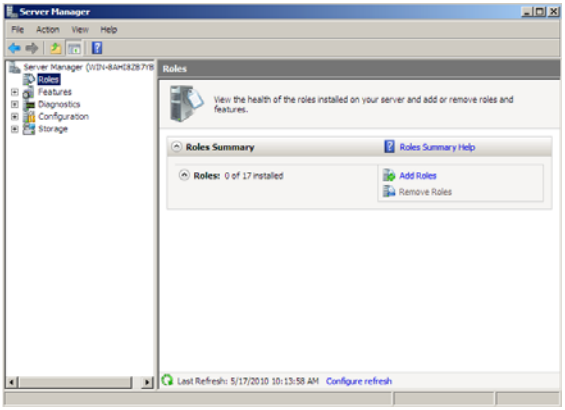
- "Installing IIS 7.0 on Windows Server 2008"
- "Installing IIS 7.5 on Windows Server 2008 R2"
- "Installing IIS 7.5 on Windows 7"

Installing IIS 7.0 on Windows Server 2008

By default, IIS 7.0 is not installed on Windows Server 2008. You can install IIS by using the *Add Roles* wizard in *Server Manager*.

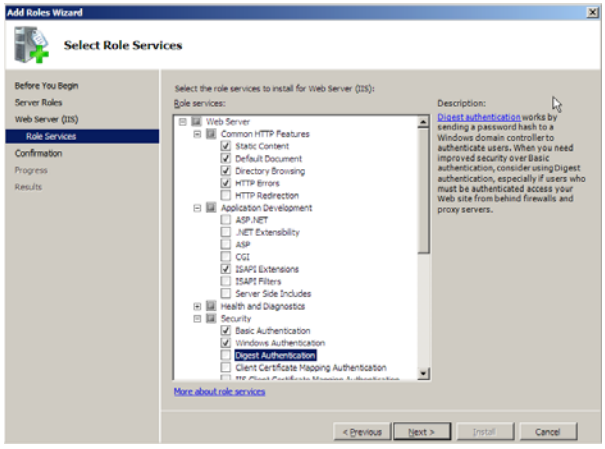
1. On the taskbar, click **Start > Administrative Tools > Server Manager** to open the **Server Manager** window.
2. In the **Server Manager** tree pane, select **Roles**.
3. In the details pane, click **Add Roles > Server Roles**.

Figure 37 Server Manager



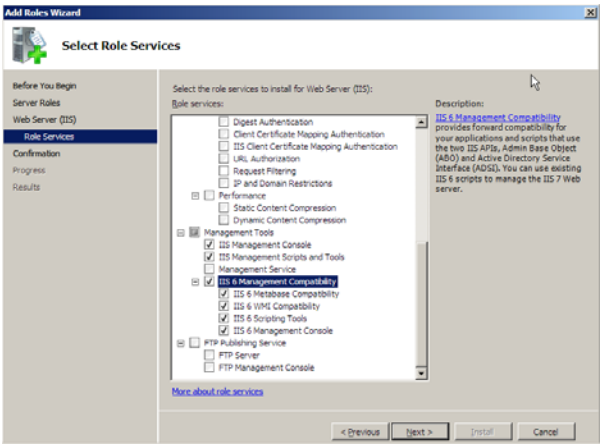
4. On the **Select Server Roles** screen, select **Web Server (IIS)**, click **Next**, and then click **Next** to open the **Select Role Services** window.

Figure 38 Select Role Services



5. Under **Roles Services**, expand **Web Server**, expand **Common HTTP Features**, and then select the **HTTP Redirection** check box.
6. Under **Web Server**, expand **Application Development** and then select the **ISAPI Extensions** check box.
7. Under **Web Server**, expand **Security**, select the **Basic Authentication** and **Windows Authentication** check boxes, and then be sure that the **Request Filtering** option is cleared.

Figure 39 Select Role Services continued



8. Under **Web Server**, expand **Performance** and then be sure that each option is cleared (*Static Content Compression* and *Dynamic Content Compression* should be cleared).
9. Under **Web Server**, expand **Management Tools,** and then select the **IIS Management Console** and **IIS Management Scripts and Tools** check boxes.
10. Under **Web Server**, expand **IIS 6 Management Compatibility** and then be sure all its options are selected.
11. Click **Next** to open the **Confirm Installation Selections** window.
12. After confirming, click **Install**.
13. After installation is complete (the **Results** window displays a successful installation), click **Close**.

After installing IIS on the server, install WebDAV Extension for IIS 7.0 (see "Installing WebDAV Extension for IIS 7.0").

Installing WebDAV Extension for IIS 7.0

1. Download the 32-bit Installation Package of the WebDAV Extension for IIS 7.0 from: http://blogs.iis.net/robert_mcmurray/archive/2008/03/12/webdav-extension-for-windows-server-2008-rtm-is-released.aspx
2. After downloading, double-click **webdav_x86_rtw.msi** to open and use the *Microsoft WebDAV Extension for IIS 7.0 Setup* wizard.

Figure 40 Setup wizard

Microsoft WebDAV Extension For IIS 7.0 Setup
Microsoft IIS Internet Information Services
Please read the Microsoft WebDAV Extension For IIS 7.0 License Agreement
MICROSOFT SOFTWARE SUPPLEMENT LICENSE TERMS
MICROSOFT WEBDAV EXTENSION FOR IIS 7.0
PLEASE NOTE: Microsoft Corporation (or based
I accept the terms in the License Agreement
Print
Back
Install
Cancel

3. After the software is installed, click **Finish**.

Configuring the Web.config File

You can modify the *Web.config* file to prevent the following errors:

- Upload fails for files larger than 30 MB.
- Merlin imaging fails when the URL and query string sizes are not adequate.

Add the following contents to the *Web.config* file (the *Web.config* file can be found in the **inetpub\wwwroot** folder):

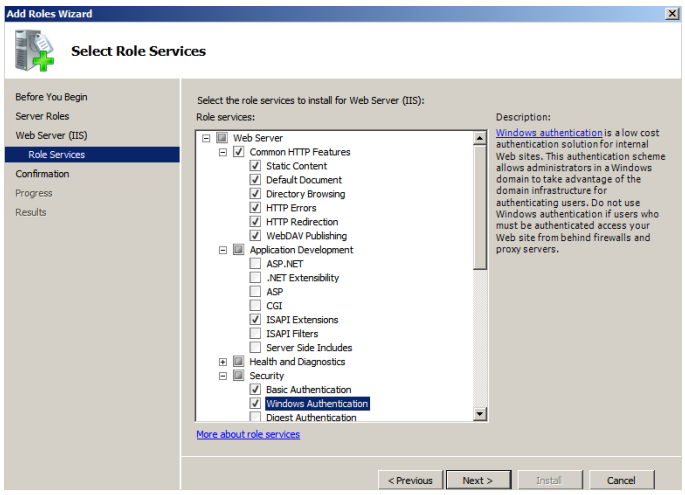
```
<security>
<requestFiltering>
<requestLimitsmaxAllowedContentLength="4294967296" maxUrl="8000"
maxQueryString="8000" />
</requestFiltering>
</security>
This example shows the web.config file with the contents added:
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
    <system.webServer>
        <directoryBrowse enabled="true" showFlags="Date, Time,
Size, Extension, LongDate" />
:
:
       <security>
 <requestFiltering>
     <requestLimitsmaxAllowedContentLength="4294967296"
maxUrl="8000" maxQueryString="8000" />
 </requestFiltering>
      </security>
    </system.webServer>
</configuration>
```

Installing IIS 7.5 on Windows Server 2008 R2

By default, IIS 7.5 is not installed on Windows Server 2008 R2. You can install IIS by using the *Add Roles* wizard in *Server Manager*.

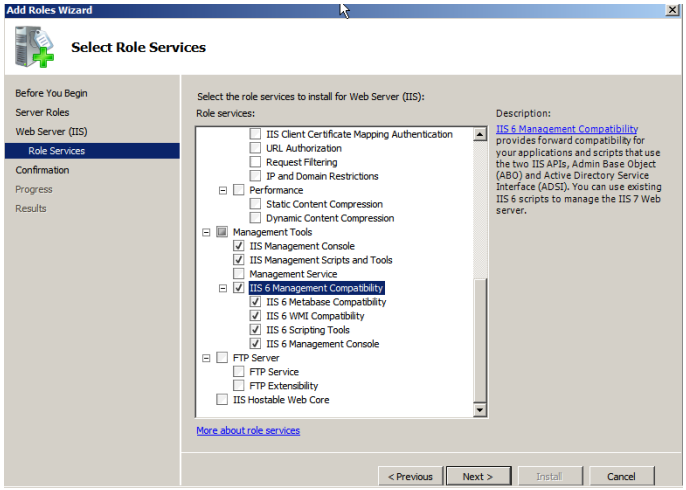
1. On the taskbar, click **Start > Administrative Tools > Server Manager** to open the **Server Manager** window.
2. In the **Server Manager** tree pane, select **Roles**, and then click **Add Roles** to open the **Add Roles Wizard** window.
3. In the **Add Roles** wizard, click **Server Roles**, and then check the **Web Server (IIS)** check box.
4. In the **Add Roles** wizard, click **Server Roles > Web Server (IIS) > Role Services**.

Figure 41 Select Role Services



5. Under **Role Services**, expand **Web Server**, expand **Common HTTP Features**, and then select the **WebDAV Publishing** check box.
6. Under **Role Services**, expand **Application Development**, and then select the **ISAPI Extension** check box.
7. Under **Role Services**, expand **Security**, select the **Basic Authentication** and **Windows Authentication** check boxes, and then be sure that **Request Filtering** option is cleared.

Figure 42 Select Role Services continued



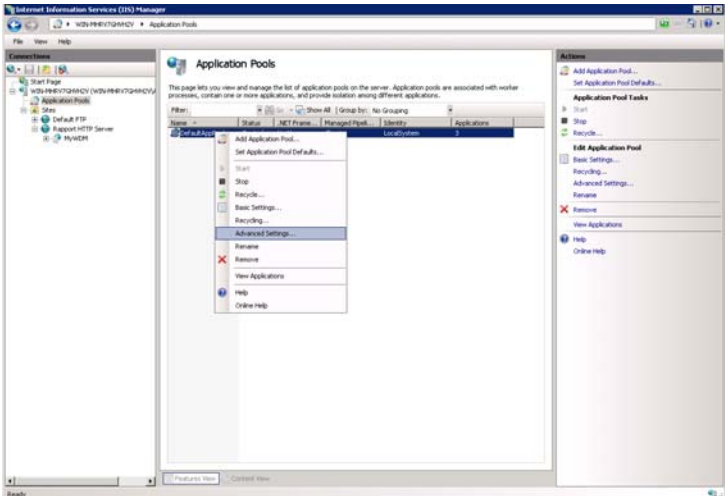
8. Under **Role Services**, expand **Performance**, and then be sure that each option is cleared (*Static Content Compression* and *Dynamic Content Compression* should be cleared).
9. Under **Role Services**, expand **Management Tools**, and then select the **IIS Management Console** and **IIS Management Scripts and Tools** check boxes.
10. Under **Role Services**, expand **IIS 6 Management Compatibility**, be sure that all options are selected, and then click **Next** to open the **Confirm Installation Selections** window.
11. After confirming, click **Install**.
12. After installation is complete (the **Results** window displays a successful installation), click **Close**.
13. After successful installation of IIS 7.5 on Windows Server 2008 R2, you must verify the following advanced settings:
    - Enable 32-Bit Applications is set to True.
    - Idle Time-out (minutes) is set to 0 (zero).

    Use the following guidelines:

    a. On the taskbar, click **Start > Administrative Tools > Internet Information Services (IIS) Manager** to open the **Internet Information Services (IIS) Manager** window.

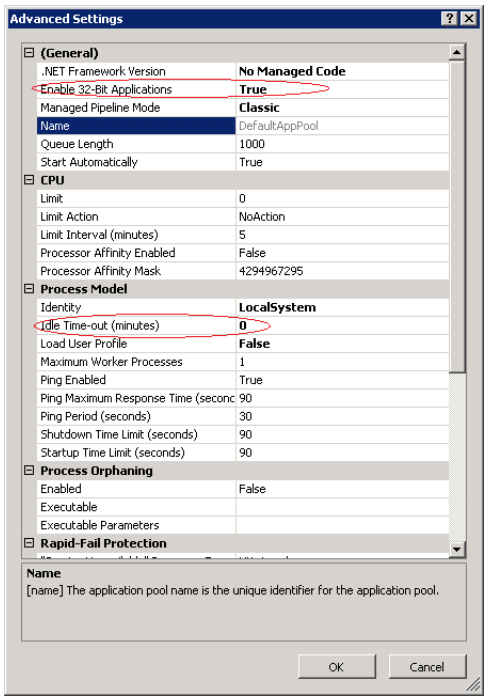
    b. In the **Internet Information Services (IIS) Manager** tree pane, expand **Server**, and then click **Application Pools** to display the **DefaultAppPool** in the *Application Pools* list.

Figure 43 DefaultAppPool - Advanced Settings



c. Right-click the **DefaultAppPool** and select **Advanced Settings** to open the **Advanced Settings** window.

Figure 44 Advanced Settings



d. In the *General* section, ensure that **Enable 32-Bit Applications** is set to **True**.

e. In the *Process Model* section, ensure that **Idle Time-out (minutes)** is set to **0** (zero)

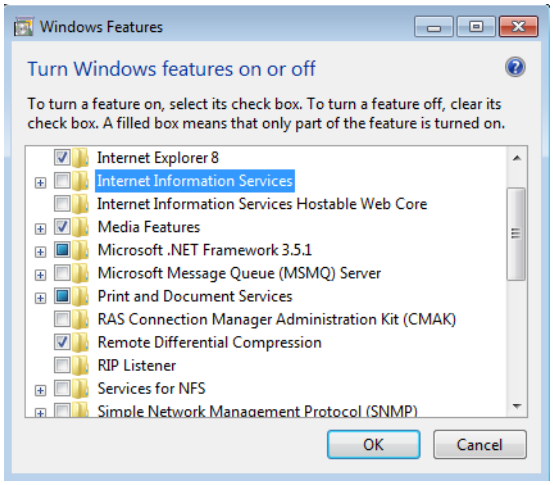
14. Continue with "Installing or Upgrading WDM Enterprise Edition."

Installing IIS 7.5 on Windows 7

By default, IIS 7.5 is not installed on Windows 7. You can install IIS by using the *Turn Windows Features on or off* wizard in *Programs and Features*.

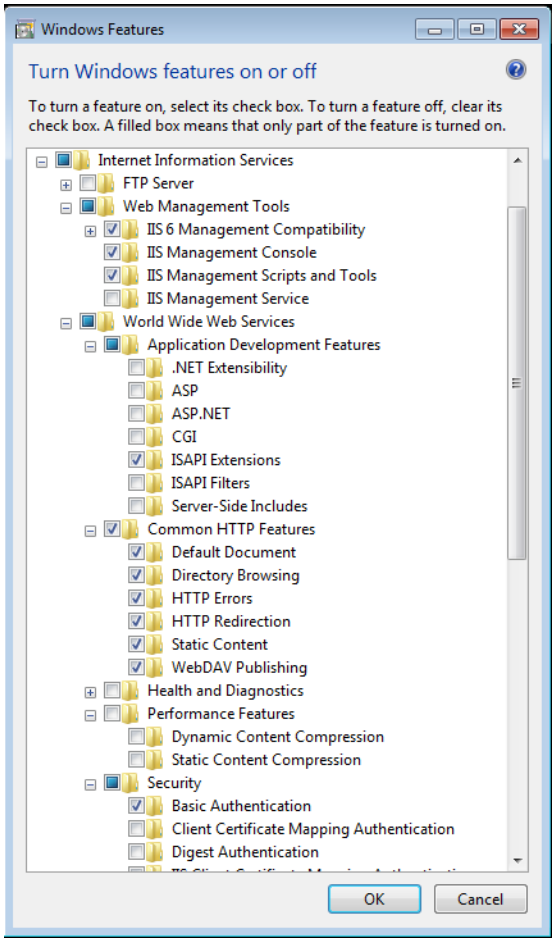
1. On the taskbar, click **Start > Control Panel** to open **Control Panel**.
2. Click **Programs > Programs and Features**, and then on the left pane click **Turn Windows Features on or off** to open the **Windows Features** window.
3. Scroll to **Internet Information Services**.

Figure 45 Internet Information Services


Windows Features
Turn Windows features on or off
To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.
Internet Explorer 8
Internet Information Services
Internet Information Services Hostable Web Core
Media Features
Microsoft .NET Framework 3.5.1
Microsoft Message Queue (MSMQ) Server
Print and Document Services
RAS Connection Manager Administration Kit (CMAK)
Remote Differential Compression
RIP Listener
Services for NFS
Simple Network Management Protocol (SNMP)
OK
Cancel

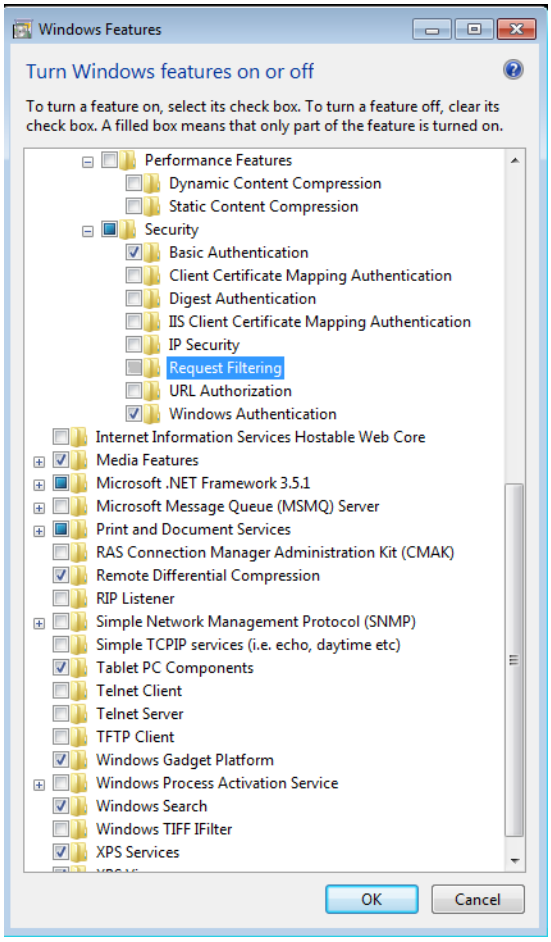
4. Expand **Internet Information Services.**

Figure 46 Internet Information Services expanded



5. Expand **Web Management Tools**, and then select the **IIS 6 Management Compatibility**, **IIS Management Console**, and **IIS Management Scripts and Tools** check boxes.
6. Expand **World Wide Web Services**, expand **Application Development Features**, and then select the **ISAPI Extensions** check box.
7. Under **World Wide Web Services,** expand **Common HTTP Features**, and then select the **Default Document**, **Directory Browsing**, **HTTP Errors**, **HTTP Redirection**, **Static Content**, and **WebDAV Publishing** check boxes.
8. Under **World Wide Web Services,** expand **Performance Features**, and then be sure all options are cleared (*Dynamic Content Compression* and *Static Content Compression* should be cleared).

Figure 47 Request Filtering



9. Under **World Wide Web Services,** expand **Security**, select the **Basic Authentication** and **Windows Authentication** check boxes, and then be sure that the **Request Filtering** option is cleared.
10. Click **OK** to install IIS.
11. Continue with "Installing or Upgrading WDM Enterprise Edition."

Using Windows Firewall with WDM

If you are using Windows Firewall with your *WDM Workgroup Edition* or your *WDM Enterprise Edition*, the WDM installer logs on as an administrator and adds the *WDM DHCP Proxy*, *WDM TFTP*, *Inetinfo*, and *Rptservicelogs* programs to the *Programs and Services* list on the *Exceptions* tab of the **Windows Firewall** dialog box (for information on adding a program to the Windows Firewall exception list, refer to the Microsoft documentation on the Microsoft Web site).

Caution

WDM Enterprise Edition ONLY - This procedure is done on each server on which you performed a WDM installation or upgrade.

This page intentionally blank.

Tables

1 Server Hardware Requirements for 32-bit OS *6*
2 Server Hardware Requirements for 64-bit OS *6*
3 Server Software Requirements *6*
4 Communication Ports *7*

Installation Guide

Wyse Device Manager™ Release 4.9.1
Issue: 042012

Written and published by:
Wyse Technology Inc., April 2012

Created using FrameMaker® and Acrobat®